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

Consultation Report

THE BOARD OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

CR03/2015	**APRIL 2015**

Copies of publications are available from:
The International Organization of Securities Commissions Web site: 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 *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity* (Consultation Report). The Consultation Report provides background on the project and the work undertaken by IOSCO's Committee on the Regulation of Secondary Markets with regard to the robustness of trading venues and their business continuity plans and recovery planning, particularly in light of market disruptions that have occurred in some IOSCO jurisdictions. This report discusses IOSCO's findings based on the responses to surveys to both regulators and Trading Venues and proposes some recommendations[1] to regulators to help ensure that they manage effectively identified risks. The report also proposes sound practices[2] that should be considered by Trading Venues in developing and implementing risk mitigation mechanisms that ensure the integrity, resiliency and reliability of their critical systems as well as their BCP. *It is recognized 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.* 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 Zhong Li, IOSCO General Secretariat, at consultation-2015-03@iosco.org
  - The subject line of your message must indicate *Electronic Trading Risks and Plans for Business Continuity*.
  - 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.

---

[1] Recommendations are results or conclusions regarding regulatory issues and approaches that IOSCO members should consider. These may or may not be incorporated, for assessment purposes, into the IOSCO *Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation* (Assessment Methodology).

[2] "In general, in accordance with IOSCO taxonomy, "sound practices" consist of practices that regulators could consider. In this report, however, we direct the sound practices to trading venues. In either case, such practices would not be reflected in the Assessment Methodology, as they do not represent a standard that IOSCO members are necessarily expected to implement or be assessed against.

- **Paper**

Send three copies of your comment letter to:

Zhong Li
International Organization of Securities Commissions (IOSCO)
Calle Oquendo 12
28006 Madrid Spain

Your comment letter should indicate prominently that it is a comment on "*Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity*."

Table of Contents

A. INTRODUCTION AND BACKGROUND

This project continues IOSCO's consideration of the impact of technology on trading.[3] The focus of this paper is on Trading Venues and how they manage technology.[4] There is general recognition that technology offers many advantages and efficiencies, such as:

- Expediting transactions in securities and derivatives by enhancing the capacity, accuracy and speed of order transmission and execution;
- Facilitating linkages of systems, including electronic trading systems;
- Enabling transactions from remote locations; and
- Enhancing the ability of market authorities to conduct surveillance and develop transaction audit trails.

Yet the benefits offered by technological developments and electronic trading should not overshadow the potential risks that these innovations can pose to the efficiency and integrity of markets, including the risks posed by errant order flow to fair and orderly markets.[5] Recent cases[6] of technological problems illustrate the risks associated with increasing reliance on technology and the inherent systemic vulnerability if electronic systems do not function properly. In addition to the key risk of potentially being unable to trade, technological problems can negatively impact overall confidence in markets, Trading Venues and participants.[7]

---

3 *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency* at p.9 (Oct. 2011), available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD361.pdf.

4 For purposes of this project, the term "Trading Venue" is generally defined as exchanges or other multi-lateral trading facilities, including, for example, alternative trading systems (ATSs) and multi-lateral trading facilities (MTFs). It also refers to the operator of a particular exchange or trading facility. IOSCO recognizes, however, that the concept of a "Trading Venue" is evolving in a number of IOSCO member jurisdictions. For example, the concept may, at the discretion of individual members for their jurisdictions only, also include swap execution facilities (SEFs) or the proposed European "organized trading facilities" (OTFs). A "Trading Venue" does not, however, include a single dealer system or a broker crossing facility.

5 Market Integrity is the extent to which a market operates in a manner that is, and is perceived to be, fair and orderly and where effective rules are in place and enforced by regulators so that confidence and participation in their market is fostered. Market Efficiency refers to the ability of market participants to transact business easily and at a price that reflects all available market information. Factors considered when determining if a market is efficient include liquidity, price discovery and transparency. *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency*, at p.9 (Oct. 2011), available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD361.pdf.

6 For example, In Mexico, a "fat finger" participant error in May 2012 posed a systemic risk to the domestic market (1.13 million shares representing US$3.78 billion were traded erroneously). In Europe, there was recently a delay in opening a market for 5 minutes because of a participant's system that was duplicating orders. The market opened with the participant entering orders manually.

7 In addition, the extensive use of technology creates challenges for regulators in the context of market monitoring, and surveillance. IOSCO discussed these challenges in its recent paper entitled *Technological Challenges to Effective Market Surveillance: Issues and Regulatory Tools* (2013). *See* http://www.iosco.org/library/pubdocs/pdf/IOSCOPD412.pdf.

Securities regulators globally have been looking at issues associated with technological developments and trading in the context of Trading Venue operations and as a result have been reviewing existing requirements or introducing requirements or guidelines to ensure that risks are being managed.[8] In addition, IOSCO has worked to enhance the ability of financial market participants to manage risks, withstand catastrophic events, facilitate the swift resumption of services in the event of disruption and help to ensure the integrity of data necessary for the resumption of normal market operations. For example, IOSCO issued reports on *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency*[9] and *Technological Challenges to Effective Market Surveillance: Issues and Regulatory Tools*[10] that discuss the mechanisms that can be used to manage widespread use of technology by Trading Venues and participants. In addition, in 2006, the Joint Forum[11] issued *High-Level Principles for Business Continuity*,[12] a report that sets out a broad framework of sound practices for all financial market participants, including Trading Venues (the Joint Forum Report). The Joint Forum's Principles are set forth in Appendix 1.

---

8 For example, in Canada, requirements relating to Trading Venue systems have been examined and amendments proposed in April 2014. On February 24, 2012, ESMA published the Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities, dealing, among others, with the resilience of trading venues and their ability to ensure fair and orderly trading through their systems. In order to strengthen the resilience of markets in the light of technological developments and building on the ESMA Guidelines, the new Directive 2014/65/EU on May 15, 2014 explicitly requires Trading Venues to have in place effective systems, procedures and arrangements to ensure their trading systems are resilient, have sufficient capacity to deal with peak order and message volumes, are able to ensure orderly trading under conditions of severe market stress, are fully tested to ensure such conditions are met and are subject to effective business continuity arrangements to ensure continuity of their services if there is any failure of their trading systems. In this respect, ESMA is required to develop regulatory technical standards to further specify the requirements for the systems and controls for trading venues. In the U.S., on November 19, 2014, the U.S. Securities and Exchange Commission adopted Regulation SCI to help strengthen the technology infrastructure of the U.S. securities markets and improve resilience when technological issues arise. Specifically, Regulation SCI requires securities exchanges and certain alternative trading systems, among other key U.S. securities market participants, to have written policies and procedures reasonably designed to ensure that automated systems that support market functions have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the entity's operational capability and promote the maintenance of fair and orderly markets. Regulation SCI also requires covered entities to, among other things, take appropriate corrective action when systems issues occur; notify the SEC of certain systems problems and systems changes; inform members and participants about systems issues; conduct testing of its business continuity and disaster recovery plans; and conduct annual reviews of their automated systems.

9 *Infra* at n.3.

10 *Infra* at n.5 and 7.

11 The Joint Forum was established in 1996 under the aegis of the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS) to deal with issues common to the banking, securities and insurance sectors, including the regulation of financial conglomerates. The Joint Forum is comprised of an equal number of senior bank, insurance and securities supervisors representing each supervisory constituency. http://www.bis.org/bcbs/jointforum.htm.

12 http://www.bis.org/publ/joint17.pdf .

As Trading Venues play an important role in the global financial system, risk controls and processes (such as microstructure thresholds,[13] change management procedures, and quality assurance processes), effective business continuity plans (BCP) become even more important. For purposes of this report, the term BCP includes disaster recovery plans (DRP).[14]

Following a number of market disruptions, the IOSCO Board asked its Committee on the Regulation of Secondary Markets to investigate their causes, identify the steps taken by industry and regulators to address them, and to consider the recommendations of the Joint Forum Report. Based on that initial inquiry, IOSCO observed the following:

- Many of the market disruptions appear to be related to technological malfunctions, and most had limited market-wide impact.
- Larger systems failures were due to hardware failures.
- Some industry representatives believe that a key risk is the complexity of the markets caused by technological advances. They therefore emphasize the importance of effective testing and controls.

To further investigate, IOSCO examined regulatory and Trading Venue requirements and policies that mitigate the risks associated with electronic trading and mitigate trading disruptions. It also examined the requirements applicable to systems and technology (*i.e.*, hardware, software and systems up-grades).

The purpose of this examination was to identify:

- the steps taken by Trading Venues in various jurisdictions to ensure proper functioning and secure access;
- the BCPs developed and implemented by Trading Venues;
- the regulatory tools used to manage the risks associated with electronic trading, ensure the robustness of systems, and the effectiveness of BCPs; and
- recent events and any lessons learned.

A survey was sent out to Trading Venues across more than 30 different jurisdictions. IOSCO also consulted and coordinated with the IOSCO Committee on the Regulation of Intermediaries (C3) to support this project. C3 surveyed those intermediaries that have electronic access to

---

[13] "Microstructure threshold" examples include single stock and/or market wide circuit breakers, along with volatility thresholds where given volume/price parameters are set.

[14] 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* the Joint Forum Report, p. 2. As noted above, BCP include DRP, which are more technical plans 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 DRP.

Trading Venues as members or subscribers (regarding their policies and automated processes and controls). For the purposes of this paper, this subset of intermediaries will be referred to as "Trading Venue participants." Approximately 40 Trading Venues and 36 Trading Venue participants responded. Characterizations in this report concerning the practices or views of Trading Venues and/or Trading Venue Participants are based upon the survey responses.

IOSCO also considered its published reports relevant to this issue,[15] along with work on cyber-crime conducted by the IOSCO Research Committee and the World Federation of Exchanges.[16] IOSCO recognizes that critical systems also exist at the central counterparty (CCP) level. However, these issues with regard to such systems have been and will continue to be considered by IOSCO within the context of its continuing work on financial market infrastructures[17] and were therefore not considered as part of this project.

This report discusses IOSCO findings based on the responses to the surveys and provides some recommendations[18] to regulators to help ensure that Trading Venues manage effectively the identified risks. The report also proposes sound practices that should be considered by Trading Venues in developing and implementing risk mitigation mechanisms that ensure the integrity, resiliency and reliability of their critical systems as well as their BCP.

In developing these recommendations and sound practices, IOSCO considered the sophistication of the Trading Venue's trading and surveillance technology, the size and complexity of the market and its inter-linkages, and the unique business needs of individual Trading Venues and market participants. These factors, as well as the size and scale of the Trading Venue, should be considered when applying the recommendations and sound practices. In addition, nothing in the recommendations or sound practices should be viewed as inhibiting Trading Venues' flexibility, nor are they intended to supersede domestic regulatory obligations.

B. TECHNOLGY-RELATED RISKS FACED BY TRADING VENUES

Trading Venues should offer the public a trading platform that can be used reliably and that fosters market integrity and investor protection. If Trading Venues experience outages, and

---

15 *Policies on Error Trades* (2005), available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD208.pdf; *Principles for Direct Electronic Access to Market*, http://www.iosco.org/library/pubdocs/pdf/IOSCOPD332.pdf; FR08/10, Aug. 2010; *Regulatory Issues Raised by the Impact of Technological Changes on Market Integrity and Efficiency;* http://www.iosco.org/library/pubdocs/pdf/IOSCOPD361.pdf, FR 09/11, Oct. 2011; and *Technological Challenges to Effective Market Surveillance: Issues and Regulatory Tools* http://www.iosco.org/library/pubdocs/pdf/IOSCOPD412.pdf, FR 04/13, Apr. 2013.

16 *Cyber-crime, securities markets and systemic risk*, Joint Staff Working Paper of the IOSCO Research Department and the World Federation of Stock Exchanges (July 16, 2013), available at: http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

17 See *Principles for financial market infrastructures* (December 2012); Implementation Monitoring of PFMIs: First update to level 1 assessment report, Report of the Committee on Settlement Systems and the IOSCO Board (May 2014), http://www.iosco.org/library/pubdocs/pdf/IOSCOPD440.pdf.

18 *See* n. 1, *supra*.

particularly if this is the result of technology not being managed effectively, investor confidence and market integrity as a whole can be negatively impacted.

Leveraging its collective experience and the key conclusions from its initial fact-finding exercise, IOSCO has identified a broad range of risks faced by Trading Venues, which may be exacerbated in an electronic trading environment. These risks necessitate the development of policies and procedures to manage systems development and changes, and the need to manage, among others, any risks posed to day-to-day operations. These risks also highlight the importance of the development of robust BCPs.

The risks identified include, but are not necessarily limited to, the following:

- *IT malfunctions and system/network failures at the Trading Venue*. Such events may impact critical systems and arise during the otherwise normal operation of systems, the implementation of new systems, or changes/upgrades to systems. This may include a hardware or software failure that impacts the operation of a venue's matching-system. Other points of possible failure include the electronic gateways that manage the incoming and outgoing flow of messages between the venue and its participants, the systems responsible for the dissemination of data and other messages (*e.g.*, confirmations), and the networks of fiber optic connectivity within the venue's data center. Risks arising from failures at third party suppliers (*e.g.*, of data centers and other systems) may give rise to similar impacts.

- *The malfunction of a trading participant's algorithms*. Fundamentally different to the risks discussed above, malfunctioning algorithms may pose a risk to the orderly operation of a venue's markets and may, *in extremis*, cause stress to the Trading Venue's systems. This may arise, for example, as a result of an algorithm malfunction that generates an excessive number of messages, thus potentially overwhelming a Trading Venue's systems' capacity.

- *Human error*. Human errors, such as fat finger errors or coding errors can be exacerbated in an electronic trading environment.

- *Risks related to "cyber crime."* Trading Venues' systems may be subject to cyber-attack. Similarly, attacks on the systems of participants may present risks to the systems of the Trading Venues on which that participant trades.

- *Risks related to the occurrence of acts of terrorism (other than cyber-attacks) or natural disasters*. The impact of acts of terrorism or natural disasters may or may not be magnified in an electronic trading environment. For example, if a natural disaster occurs where a primary site of a Trading Venue is located, being fully redundant in another location may mitigate, not exacerbate, the impact.

- *Legal/compliance/reputational risk* from material, prolonged and/or repeated systems outages.

- *Potential liquidity/transparency risks.* Should a Trading Venue fail to mitigate electronic trading risks, resulting in trading disruptions, trading may move to other markets. The movement of trading to other venues with better risk management is not a negative development *per se*, particularly in those jurisdictions with multiple markets. However, if sufficient alternative domestic Trading Venues do not exist, this may result in a movement of trading outside the jurisdiction.

In examining these risks, both regulators and Trading Venues have focused on critical systems, in particular, how to identify and then protect them from external threats and what to do when they are disrupted. The sections that follow discuss these critical systems.

C. DESCRIPTION OF CRITICAL SYSTEMS

In general, the term "critical systems" for purposes of this report refers to all computer, network, electronic, and technological systems that directly support trading operated by or on behalf of the applicable Trading Venue, including order routing, market data, market regulation, or market surveillance. Many regulators themselves do not use a specific definition of "critical system" when regulating Trading Venue systems or reviewing BCPs.[19] Some regulators have identified critical systems or are proposing to do so.[20] In addition, certain jurisdictions may identify in their regulations specific critical systems that merit a higher level of oversight and attention.

Based upon the answers to the IOSCO survey, Trading Venues are generally consistent in what they identify as critical systems. Depending on the services provided by the Trading Venue or the type of Trading Venue (equity vs. derivative), however, the services identified below may or may not be considered by the Trading Venue as one of its critical systems.

---

[19] For example, in Europe, article 48 of Directive 2014/65/EU requires Trading Venues to establish effective contingency arrangements to cope with the risk of system disruptions, which in turn allows European regulators to consider this requirement as an implicit reference to identify the critical systems for Trading Venues.

[20] For example, Singapore has specifically defined a "critical system" to be a system, which in the event of failure, will cause significant disruption to the operations of the financial institution or materially impact the financial institution's service to its customers, such as a system which processes transactions that are time critical or provides essential services to customers. ESA (Hessen) regulator in Germany classifies a critical system as one that supports critical business processes. The FSA in Romania is currently proposing the definition of "critical infrastructure" to be a system or a component of a system, an essential IT infrastructure for maintaining financial infrastructure functions, to which a disturbance significantly affects its proper functioning with significant impact as a result of failure to maintain these functions. In Canada, the regulators consider systems that support order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing to be critical (see NI 21-101, Part 12. In a similar vein, the SFC in Hong Kong considers trading systems, clearing systems, price dissemination systems and the payment system linking banks and clearing houses to be critical. In India, stock exchanges, clearing corporations and depositories are considered critical infrastructure. SC Malaysia is also proposing to establish a definition of trading venue's critical system (*e.g.*, trading, clearing and depository systems) based on the material impact to the market and market participants and significant disruption of the operations, services and ability of the Trading Venue to discharge its duties sand obligations, if those systems are unavailable in the event of a disruption. In the U.S., Regulation SCI defines "SCI Systems" and "Critical SCI Systems." *See* Rule 1000.

1. *Execution Systems*

   Trading Venues in many jurisdictions consider systems related to the execution of trades, such as trading platforms and matching engines to be critical. These systems match and execute orders sent to the Trading Venue and are considered to be critical because their failure would cause a trading interruption. The risks associated with an interruption to these systems would include the inability to trade, negative impact on reputation, and a loss of confidence in the market.

2. *Data Dissemination Systems*

   Systems related to data dissemination are also considered to be critical by many Trading Venues. These systems deliver order and trade information and provide the market with real-time and historic trading-related data. These systems are considered critical because their failure would prevent market participants, including investors, from having information to make informed trading decisions. In addition, data dissemination is mandated under regulatory requirements in some jurisdictions.

3. *Network Infrastructure Systems*

   Some Trading Venues consider network infrastructure systems, such as database management systems, storage systems, switches, firewalls and network connections as critical systems because they support other critical systems such as execution systems and data dissemination systems. If a Trading Venue's network infrastructure systems fail, other critical systems may be impacted.

4. *Surveillance Systems*

   Surveillance systems are also considered to be critical and may include surveillance data feeds sent directly to regulators, along with systems used to monitor trading. Trading Venues may, in some jurisdictions, be prohibited from operating without appropriate surveillance.[21]

5. *Risk Management Systems*

   Also critical are risk management systems such as pre-trading limits, drop copies that allow participants to monitor trading activity, risk-based margining systems and market maker protection tools. Some Trading Venues consider these systems to be critical as they help mitigate the financial and regulatory risks of electronic trading for participants.

[21] In some cases, if a real-time surveillance system is not functioning properly, but surveillance alerts can be run at the end of business or a later date, a Trading Venue may be permitted to continue to operate.

6. *Order Entry Systems*

   Order entry systems allow orders to be sent to the execution system and as a result are critical to the operations of a Trading Venue. A disruption of these systems may result in the inability to submit orders and an interruption in trading.

7. *Order Routing Systems*[22]

   Order routing systems may be critical in jurisdictions that have multiple venues. These Trading Venue systems enable the routing of orders by the Trading Venue away from the Trading Venue to other Trading Venues. They do not, in this context, include systems used by intermediaries to route orders to Trading Venues.

8. *Other Systems*

   There are a host of additional systems that may be critical to a Trading Venue. Specifically, some Trading Venues identified as critical the systems that support the proper clearing and settlement of trades. These systems supply information of executed trades to clearing agencies, and some Trading Venues indicated that a disruption of these systems would adversely affect proper clearing activity, which can comprise a major function of the Trading Venue or the market.[23]

   In addition, some Trading Venues expressed the view that data center providers that host Trading Venue servers, power, Internet and telecommunication services are also critical because their failure could lead to a possible trading disruption. However, many of these are beyond the focus of this paper as they are generally systems that are not within (and have never been imputed to be within) the control of the Trading Venue and are not subject to oversight by securities regulators.

The remainder of this report focuses on what steps both regulators and Trading Venues have taken to ensure that a Trading Venue's critical systems are protected and that if there is a disruption, the Trading Venue has a plan to continue its business operations. As noted earlier, in this report IOSCO proposes a set of recommendations to regulators regarding mechanisms to protect critical systems and the creation of BCPs. Based upon the practices we identified from the Trading Venues that responded to the IOSCO survey, IOSCO developed a set of sound practices that all Trading Venues should consider both with regard to the protection of their critical systems and the components of their BCPs.

---

22 As distinct from order entry system facilitating the entry of orders into a trading engine, the goal of order routing system is to re-route orders from a Trading Venue to another Trading Venue.

23 Despite this, as noted above in Section A, clearance and settlement systems are outside of the scope of this paper.

D. MANAGING TECHNOLOGY TO MITIGATE RISK

Reliance of Trading Venues on technology necessitates that the Trading Venue ensure that its technology and critical systems remain resilient and reliable. The systems and services also need to have integrity so that confidence in the operations of the Trading Venue is maintained. This is accomplished by having mechanisms, policies, procedures and processes in place that, among other things, ensure that existing systems operate effectively and securely, and controls for when the Trading Venue introduces or makes changes to critical systems. In this regard, regulatory authorities have also recognized the need for Trading Venues to appropriately monitor critical systems and have appropriate control mechanisms in place.

There are many different mechanisms that Trading Venues and regulators use or require to ensure the resiliency (including robustness), reliability and integrity of critical systems, including controls around how the Trading Venue introduces changes and manages its critical systems. Other mechanisms are built into the Trading Venue systems to identify and manage external risks, such as errors by participants or errant algorithms. These types of mechanisms include pre-trade controls, circuit breakers, and kill switches. Trading Venues also have BCPs and DRPs as mechanisms to help them prepare for serious disruptions and have clarity as to the steps to be taken for recovery. Microstructure mechanisms to manage external risks to critical systems such as circuit breakers are discussed in Part E and BCP and DRP are discussed in Part F.

This section outlines the steps taken to ensure integrity, resiliency and reliability and how Trading Venues manage the introduction of new or changes to its critical systems.

1. Governance

Effective governance is key in the management of critical systems. At many Trading Venues, senior management plays an ongoing decision-making role with respect to critical systems, as well as in the review and approval of policies and compliance with regulatory requirements. However, organizational hierarchies in Trading Venues are highly diverse and not uniformly comparable. As a result, the layers of governance, and who performs what role, may differ significantly amongst Trading Venues.

Day-to-day responsibility for Trading Venue technology and operations often falls to the Chief Information Officer (CIO) and/or the Chief Operations Officer (COO). However, the Chief Executive Officer (CEO) often has ultimate responsibility for managing the processes and decisions concerning the venue's critical systems.

At the operational level, it is common for Trading Venues to use separate teams for systems development, user acceptance testing, systems' roll-out/deployment and quality assurance of trading infrastructure. This separation of responsibilities can help to maintain independence between processes and detect mistakes. In addition, external IT auditors are retained by some Trading Venues to assist with the testing of systems.

In the context of the governance of critical systems, where there is an incident, Trading Venues often assign a specific role of "incident manager" to individuals (often business managers) so that they have a central person who is accountable in the event of an incident. This person may or may not be the same person that manages or is accountable for BCP or DRP implementation.

Incidents that occur may or may not be severe enough to trigger BCP or DRP. Risk committees, business managers or senior management may make this determination. The discussion relating to the governance of BCP and DRP is discussed below. Most Trading Venues advised that their escalation procedures, which include reporting to senior/executive management, vary depending on the severity of the incident. In certain cases, a crisis would be escalated to the Board.

2. IT skills

With regard to the IT skills needed to manage and operate critical systems, most Trading Venues seek to recruit persons with relevant skills and experience for these roles. Generally, Trading Venues often view relevant industry knowledge and on-the-job training/assessment as being more relevant requirements than formal qualifications, although some Trading Venues require their staff to obtain/maintain training certifications.[24] It also appears that most Trading Venues provide in-house training for their relevant staff, and some require staff to undergo periodic tests to ensure that they keep their required knowledge up-to-date.

3. Ongoing monitoring of critical systems

Where regulatory frameworks are in place relating to a Trading Venue's monitoring and ongoing testing of critical systems, the approach varies. Some jurisdictions do not impose specific regulatory requirements regarding the ongoing monitoring of Trading Venue systems because, in their view, Trading Venues must do so anyway as a practical matter in order to satisfy regulatory requirements to give notice of disruptions or incidents.

Some jurisdictions impose general obligations for Trading Venues to have appropriate measures in place to handle risks. Other jurisdictions impose specific requirements (or provide guidelines[25]) that require (or recommend) that Trading Venues:

---

[24] For example, Trading Venues identified as relevant standards ISO22301: 2012 (business continuity), ISO27000 series (information security related certifications) and BS25999-2:2007 (business continuity management).

[25] In addition to the ESMA guidance referenced above in footnote 9, Directive 2014/65/ EU (MiFID II) will further develop the ESMA guidance and require Trading Venues to have in place effective systems, procedures and arrangements to ensure their trading systems are resilient have sufficient capacity to deal with peak order and message volumes, are able to ensure orderly trading under conditions of severe market stress, and are fully tested to ensure such conditions are met. CFTC rule 38.150 implements the Commodity Exchange Act's Core principle requiring designated contract markets to maintain a program of risk analysis and oversight to identify and minimize sources of operational risk. CFTC rule 38.1051 requires such a program to address specific categories of risk analysis and oversight: information security; business continuity-disaster recovery planning and resources; capacity and performance planning; systems operations; systems development and quality assurance; and physical security and environmental controls. *See also* CFTC rule 37.1400, which implements similar requirements for swap execution facilities (SEFs). In India, SECC Regulations mandate stock exchanges to maintain adequate systems' capacity supported by

- maintain adequate internal controls over their critical systems;[26]
- submit monthly statistics on systems performance;[27]
- set benchmarks against which to measure operational effectiveness and efficiency;[28]
- monitor and review indicators such as performance, capacity and utilization;[29]
- conduct regular systems reviews; and
- monitor electronic trading systems on a regular basis to identify and remedy deficiencies, and to ensure that there is an appropriate governance process in place, including procedures for the sign-off of resolution of problems identified through monitoring.[30]

To ensure critical systems resiliency, Trading Venues use policies and procedures respecting capacity and performance management, including stress testing, to measure systems limitations based on current architecture and to monitor if limits are being approached. To ensure systems integrity, information security policies are maintained, BCPs and DRPs are established, and production management and change management policies are followed.[31] Use of system development methodologies that divide work into distinct phases in order to better manage work flows seems to be employed by most Trading Venues.[32] In addition, application controls[33] are used to ensure the reliability and integrity of data entered and processed by critical systems.

A number of Trading Venues set metrics that are used to measure system performance and capacity. These Trading Venues frequently monitor the metrics to track key performance indicators, to monitor traffic volumes and generate capacity indicators in the trading system. A number of Trading Venues use alerts that trigger warnings related to performance or stability ratings of the trading systems or that provide notice when pre-established capacity thresholds are breached, and these are monitored across a spectrum from a constant basis to a weekly basis.

---

a business continuity plan, including a disaster recovery site. Detailed guidelines on BCP and capacity planning have been provided to the stock exchanges.

26 Canada, India, Malaysia, Singapore, US SEC.

27 Hong Kong, Japan, Malaysia.

28 Malaysia.

29 India, Malaysia, Singapore, US SEC.

30 ESMA Guidelines on systems and controls in an automated trading environment for trading venues, investment firms and competent authorities.

31 BCP and change management, discussed below.

32 For example, a number of Trading Venues maintain a software development life cycle (SDLC) process as a tool to manage reliability of critical systems. A SDLC is essentially a series of steps, or phases, that provide a model for the development and lifecycle management of an application or piece of software. Common methodologies used in the SDLC include waterfall, spiral development and prototyping.

33 Application controls are controls over input, processing and output functions. They ensure completeness and accuracy of data.

Many Trading Venues have established formal capacity planning exercises in order to ensure resiliency and availability of critical systems. Typically, these formal exercises occur at least once per year. In some cases, these can occur as frequently as quarterly.

4. Systems reviews

Most Trading Venues conduct systems reviews of their critical systems.[34] Indeed, some jurisdictions *require* annual[35] or periodic[36] systems reviews. The majority of Trading Venues surveyed conduct a system review annually, even if not required to do so, while a small minority of Trading Venues advised that the frequency of their systems reviews is determined by the outcome of their annual risk assessment rather than by regulatory requirements.

Many Trading Venues referred to these reviews as IT-focused risk-based reviews that often encompass the entire technology infrastructure of the organization. The systems reviews cover many areas including technology infrastructure, internal controls and application controls. The reviews typically include general IT controls and processes such as change management,[37] problem management, and systems lifecycle processes. They may also include an examination of processes relating to security, governance, accountability and sign-off. In some cases, the review includes all business continuity and disaster recovery planning. The review or audit may be performed in accordance with audit standards and reported to the board of the Trading Venue and regulator.

In practice, systems reviews are performed either by a third party auditor that is not affiliated with the Trading Venue, or by an internal audit team. Many Trading Venues that use an internal audit team frequently engage external consultants to perform specific testing or reviews. Most Trading Venues that outsource critical systems require their supplying firms to operate in accordance with the Trading Venue's internal audit plan.

Where deficiencies are identified by the system review, Trading Venues determine what steps are necessary to address them.

5. Incident management

---

34 There are a wide variety of standards upon which the independent systems reviews are based. For example, COBIT framework 5.0; ISO standards 20000, 27001, 22301, 9001; CPA s.5025.

35 Canada, India.

36 Australia, Brazil, France, Hong Kong, Ireland, Italy, Malaysia, The Netherlands, Romania, Singapore, Spain, Turkey, United States (CFTC and SEC) and UK.

37 Change management is the process for controlling the lifecycle of all changes, enabling beneficial changes with minimum disruption of IT services. Problem management is the process for management of all problems that proactively prevents incidents from occurring and minimizes the impact of incidents that cannot be prevented. The systems development life cycle is the process of planning, creating, testing and deploying information systems. This concept applies to a range of hardware and software configurations.

Incident management procedures are followed when there are systems malfunctions or disruptions. These technological procedures relate to the issue that has caused the incident to occur.[38] Incident management procedures outline steps to be followed when an incident occurs, reporting procedures to management, the board or regulators, escalation and internal and external communication protocols. These procedures may in fact mirror BCP procedures, but may not, depending on the severity of the incident, trigger the BCP itself. To determine the severity of an incident, Trading Venues often classify (or "rank") an event according to business impacts, in order to prioritize and initiate appropriate responses. This will determine whether it is necessary to trigger the BCP.

The majority of regulators require Trading Venues to notify them about incidents that impact critical systems.[39] However, in some jurisdictions, only notification about material or significant incidents is required.[40] The definition of materiality varies slightly across these jurisdictions[41] as well as the timing. In general, however, required information includes a post mortem report regarding each IT incidents, which usually describes the cause of the incident, immediate remedial action taken and measures considered and implemented for preventing a reoccurrence.

6. Controls around the development of new or changes to critical systems

---

38 These are different from crisis management procedures that address broader issues associated with the occurrence of a crisis that impacts an entire organization. Crisis management procedures may also trigger BCP if appropriate in the circumstances.

39 For example, in Australia there is an obligation to notify ASIC immediately of any system issues. Brazilian regulators require Trading Venues to immediately inform the regulator about any event that affects the regular functioning of the market, even if the disruption is only temporary. In Japan, the trading venues are required to report the fact that disruption occurred immediately to the JFSA and report the outlines, causes, actions to have addressed and areas to be improved on the disruption to the JFSA without delay. Malaysian regulators require Trading Venues to notify them of all incidents relating to its operations or its stakeholders' operations or any system intrusion. In Mexico, Trading Venues are required to provide notification to the CNBV about any disruption. Singapore MAS requires Trading Venues to notify them within an hour of the discovery of an incident. In South Africa, there is a requirement to inform the FSB immediately of any matter that may pose systemic risk to the financial markets. In the UK, the Trading Venue is required to inform the FCA about any disorderly trading condition. In the United States, CFTC rules require a contract market to notify CFTC staff "promptly" of all electronic trading halts and significant systems malfunctions; cyber security incidents or targeted threats that potentially jeopardize automated system operation, reliability, security or capacity; and activation of the market's business continuity disaster recovery plan. *See also* US SEC Regulation SCI.

40 Canada, Hong Kong, India, Spain and Turkey.

41 In Canada, Trading Venues are required to promptly notify the regulator when there is a material systems failure, malfunction or delay for each of its systems that support order entry, order routing, execution, trade reporting, trade comparison, data fees, market surveillance and trade clearing (trading related systems). Similarly, in Hong Kong, Trading Venues are required to report any material failure, error or defect in the operation or functioning of their systems or equipment, and any major operational disruption. In India, all disruptions/trading halt/malfunctions to the trading systems are to be reported by the stock exchange to its Board, along with the details of the remedial measures taken to prevent occurrence of such incidents in future. Reports on all such disruption of more than five minutes are also to be provided to the Regulator (SEBI).

In addition to the need to have policies and procedures regarding the ongoing monitoring of critical systems for resiliency, integrity and reliability, the introduction of new or changes to systems requires controls.

Many regulatory authorities have introduced specific requirements and guidelines regarding the introduction of new systems and changes to existing systems,[42] although there are some that do not.[43] The approaches adopted include requirements for testing, including stress testing, as well as launch protocols, re-certification by third parties, communication protocols and providing a testing environment.

A few jurisdictions have required Trading Venues to have appropriate project management frameworks and governance frameworks regarding product development, project deliverables, timeframes and success factors. These requirements facilitate an orderly development and rollout of new (or changes to) systems. The specific expectations of regulators on the processes may be determined by the size of the Trading Venue's market, the complexity of trading, and the number and type of market participants in the market. Requirements or guidance may cover testing arrangements, stakeholder communications, definition of roles and responsibilities of staff, identification of critical success factors, milestones and deliverables, and procedural mechanisms for sign off on development, deployment and updates for new systems and changes to existing systems.

A large majority of Trading Venues treat changes to critical systems in the same manner in which they treat the development and introduction of new critical systems and have instituted extensive policies and procedures to manage these changes. These change management processes include launch protocols, capacity planning, stress testing, the use of testing environments, certification processes, monitoring of systems, and policies regarding internal coordination. They also consider and manage the impact of new or changes to critical systems on participants.

---

[42] Australia, Canada, France, Italy, Japan, Malaysia, Singapore, Spain, The Netherlands, Singapore, and UK. Many European jurisdictions cite the ESMA Guidelines. Hong Kong examines approaches in the review and approval of rules. In Japan, Trading Venues report on systems changes periodically. South Africa relies on the general principle that a Trading Venue must have arrangements to implement effective and reliable infrastructure to ensure trading is facilitated in a fair, efficient and transparent manner and contribute to the maintenance of a stable financial market environment while reducing systemic risk, combined with moral suasion.

[43] In Malaysia, the SC noted that Trading Venues will have their own implementation team, comprising the Project Steering Committee, and Project Management Committee, to monitor the implementation of new systems and, will have vendor staff either onsite or offsite on call during the implementation stage as well as during the monitoring period of the performance of the new system changes. In addition, the SC requires a post implementation review to be conducted within six months after the launch to assess the business benefits, identify risks, strength, shortcomings and completeness of the implementation and to highlight and address any issues noted during the period. The report is also required to be shared with the SC. Similarly, in Australia, the ASIC noted that the Trading Venues will have their own implementation team to monitor the new system changes and will generally have vendor staff either on site or on call (depending on the nature of the change) while the performance of new changes are being monitored. European respondents referred to the ESMA Guidelines on monitoring, which provides for real-time, periodic and holistic review of systems to identify and remedy deficiencies.

Trading Venues use change management processes as a fundamental part of their technology governance program to maintain the integrity of critical systems. The change management process is intended to provide a structure for approving (or rejecting) and implementing changes to the production environment (*i.e.*, the live trading environment), as well as to formally track, with supporting documentation, compliance with required procedures.[44] Changes that follow this process may be planned (*e.g.*, software upgrades or operating system maintenance) or unplanned (*e.g.*, a fix to a problem detected in the production environment).

Typically, production changes are made during non-trading hours. However, critical incidents can require a change to be made to the production environment during trading hours, but only on an exceptional basis. Production environment access is typically limited to select teams in the Trading Venue's IT department.

Trading Venues use extensive testing when new, or changes to existing systems are introduced. They use testing cycles and multi-layered testing processes that typically include the following tiers:

- development (to execute functional testing);
- quality assurance (both functional testing to ensure the new release works as expected, and non-functional testing in a production-like environment to perform capacity and availability testing);
- user acceptance testing (to validate system changes before they are upgraded to production environment); and
- certification (to test the new release with external customers, typically in a non-production environment).

With respect to communicating changes to market participants or the public, in most jurisdictions, Trading Venues are not subject to formal requirements. However, some jurisdictions have imposed requirements or guidelines in relation to the timing, nature and scope of communications to Trading Venue participants. These requirements may include minimum notice time for testing and the provision of revised specifications, or the need to consult with participants.[45]

---

[44] For example, one Trading Venue cited the use of a dedicated "change management committee" to review and approve all critical changes scheduled for deployment.

[45] For example, a few regulators have outlined specific requirements with regard to the communication of new critical systems to help ensure sufficient lead-time is available before such systems are launched or material changes made. For example, the JFSA requires Trading Venues to provide details and consult with the public on their system changes. SC Malaysia also requires Trading Venues to engage its participants on system changes to ensure awareness of the impact of the new system to participants' IT infrastructure. In Canada, new Trading Venues are required, at a minimum, to provide participants the specifications three months prior to launch (and two months for testing). In addition, the launch protocol requires existing Trading Venues to provide reasonable notice for the implementation of material system changes. In Hong Kong, the SFC takes into consideration the communication plan when evaluating the proposed changes, including whether major stakeholders have been consulted, adequate details have been

Even when not subject to mandatory communication requirements, many Trading Venues stressed the importance of open and regular communication with market participants throughout the process of development and testing of new critical systems. This means providing market participants with sufficient lead-time to help ensure that they are able to assess the system or the change and its impact on themselves and the market. This impact could include costs imposed for technology changes or changes in business models to incorporate new trading methodologies.

Thus, in practice, market participants, as part of the launch protocols for new systems, are usually provided notice several months' in advance of implementation to provide sufficient time for assessing the impact on their systems or operations, undertaking testing and to adapt to the systems and operational changes. For many of these Trading Venues, these communications protocols are formalized into policies and procedures. For example, some Trading Venues' policies and procedures provide that certain communications be made to market participants 60-90 days prior to implementation. A number of Trading Venues regularly communicate information regarding systems changes through their Web sites.

Many regulators also require that Trading Venues provide notification to the regulator about material changes to their systems (both in relation to the introduction of new systems and changes to existing systems).[46] This may be done through formal reporting requirements that may specify the information that must be filed. For example, Trading Venues may be required to describe the approach to managing the change, key project milestones and their preferred dates, risk management, communication to the market, and the anticipated impact on capacity, resiliency, market participants and the wider market.

The filing of information may come in the context of a formal "filing," which may be reviewed and subject to approval or non-objection by the regulator. In other jurisdictions, the reporting may be on a periodic basis or ad hoc. In one jurisdiction, Trading Venues are required to provide periodic updates during the implementation stage to keep the regulator up to date on progress.[47] This may be done on a voluntary basis or on request in other jurisdictions.

7. Outsourcing

Most Trading Venues do not outsource the operation of critical systems. Those that do may benefit from lower costs of performing a particular function while giving them access to a high level of expertise and the latest technology. Outsourcing may raise a number of issues and, while not transferring regulatory responsibility, may in certain cases transfer operational responsibility for those critical systems that have been outsourced to third parties. That being said, even where

---

provided to participants, and briefing sessions have been held with participants. In Malaysia, Trading Venues are required to provide briefing and information to stakeholders.

46 For example, see the ESMA guidelines. In addition, CFTC rule 38.1051(f) requires designated contract markets to provide CFTC staff with "timely advance notice of all material planned changes to automated systems that may impact the reliability, security or adequate scalable capacity of such systems; planned changes to the market's program of risk analysis and oversight. *See also* US SEC Regulation SCI.

47 Malaysia.

outsourcing occurs, the Trading Venue is responsible for the operations of its critical systems and compliance of those operations with regulatory requirements.[48]

A large number of Trading Venues identified "data centers" as being a critical system that they outsource.[49] In addition, a number of Trading Venues indicated that they outsource systems related to execution systems, data dissemination systems, clearing and settlement, network services and central counterparties. Less common, but also mentioned as outsourced systems that some Trading Venues thought were "critical" include hardware, hardware support services, Web hosting services, storage, equipment, and procurement services.

When Trading Venues have outsourced critical systems, and changes to those systems or new systems are introduced, it is important for them to have policies and procedures in place to ensure that system modifications do not pose risks to the orderly functioning and integrity of the venue. IOSCO's Outsourcing Report contained a number of principles.[50] One of the principles states that "there should be a legally binding written contract between the outsourcing market and each third party service provider, the nature and detail of which should be appropriate to the materiality and nature of the outsourced activity to the ongoing business of the outsourcing market." This is often covered in a Service Level Agreement (SLA) between the Trading Venue and the supplying firm.

SLAs typically outline the policies and procedures the supplying firm is required to follow, as well as the expected service levels relating to the provision, monitoring and development of the supplied service, including the committed availability[51] of the system. The SLA may also address problem reporting, incident management, management escalation and penalty clauses.[52]

---

48 In July 2009, IOSCO issued a report entitled *Principles on Outsourcing by Markets* (Outsourcing Report), available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD299.pdf. The Outsourcing Report identified activities that IOSCO considers to be core activities. These include the provision and daily operation of trading facilities, the management of the market functioning (including market surveillance and monitoring), the enforcement of exchange rules/self-regulation, post-trade services (such as clearance and settlement), trade information disclosure, product development, IT operations, admission of members authorized to trade, authorizing the trading of specific securities on the market, and the management responsibilities (function) of a Board. IOSCO states in that report that, with limited exceptions, the outsourcing market, its management and its governing body generally retain full legal liability and accountability to the market authority for any and all functions that the market may outsource to a service provider to the same extent as if the service were provided in-house. In this regard, the relevant market authority may impose sanctions and penalties on regulated markets in its jurisdiction for violations of statutory and regulatory requirements that resulted in whole or in part from the failure of a service provider (whether regulated or unregulated) to perform its contractual obligations for the outsourcing market.

49 As stated above, a number of Trading Venues identified "telecommunication" as a "critical" outsourced system, but this falls outside of IOSCO's understanding of "core" systems for outsourcing purposes. In other words, the 2009 Outsourcing principles would not apply to a Trading Venue's use of telecommunications systems, such as telephone and the Internet. See above note.

50 Those principles are set forth in Appendix 2.

51 This term generally refers to a supplier's agreement to keep the system "available" for a percentage of time.

52 If problems with individual services become persistent or are not addressed within the SLA, escalation to a "supplier account management team" typically occurs. If an issue is of a sufficient severity, Trading Venues will typically enter into an "improvement plan" with the supplying firm.

The SLA also sets out policies and procedures relating to new or changes to systems provided to the Trading Venue. Its terms often include formal and detailed testing processes prior to release, requiring the Trading Venue's approval prior to implementation, a requirement of thorough communication (continual interaction, weekly reporting, and confirmation), testing to ensure integrity of the outsourced systems with the Trading Venues systems, and requiring that the supplying firm employ the same protocols that the Trading Venue would have, had it introduced new systems or made changes to existing systems.

8. Recommendation and sound practices

Upon reviewing the current requirements and/or guidelines of regulators and the processes and procedures implemented by Trading Venues to ensure the resiliency, reliability, and integrity (which includes security) of critical systems, IOSCO makes the following recommendation to regulators. IOSCO also lists a number of sound practices that should be considered by Trading Venues as a means to ensure the resiliency, reliability and integrity, including security, of their critical systems.

As noted earlier in this report, nothing in the recommendation or sound practices restricts Trading Venues' or regulators' flexibility, and they do not override domestic regulatory obligations. Regulators have the discretion to determine whether to implement this recommendation relating to the resiliency, reliability and integrity of critical systems with respect to a particular Trading Venue or category of Trading Venues within its jurisdiction, *e.g.*, based upon size and scale (such as trade volume) or products traded.[53]

Recommendation 1 to Regulators

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

Sound Practices for Trading Venues

IOSCO has identified, through the review of current Trading Venue processes and procedures, the following sound practices that it believes all Trading Venues should consider[54] as a means to ensure the resiliency reliability and integrity, including security, of their critical systems. They are intended to allow for a wide range of application and adaptation in different jurisdictions. Subject to the regulatory requirements in its jurisdiction, it is within an individual Trading Venue's discretion to determine which may be appropriate for them.

---

[53] The IOSCO Methodology specifically recognizes that different types of trading venues may be regulated in different ways within a jurisdiction. As noted in the methodology ""[*d]ifferences related to the type of service provided, product traded and participants in the market are generally accepted bases for drawing appropriate regulatory distinctions.*" P. 199.

[54] National regulators may require all (or some) Trading Venues subject to their jurisdiction to comply with one or more of these practices. Nothing in this section should be interpreted to suggest that these regulators should change such requirements.

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.[55]

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.

[55] In general, the model should be proportional to the complexity of, and risks to, the Trading Venue's systems and describe responsibilities for decision-making, escalation and communication for incidents and crises, including those crises that trigger BCP.

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.

E. MANAGING EXTERNAL RISKS TO CRITICAL SYSTEMS

Some of the risks that might impact critical systems may originate from outside of the Trading Venue. These include risks relating to malfunctions with participant systems, errors entered by Trading Venue participants or their clients, and cyber-security breaches. We discuss below these risks, the relevant regulatory requirements, and the ways that Trading Venues seek to manage them.

1. Risks posed by access to Trading Venues

Technology used by market participants who access Trading Venues can introduce risks to the Trading Venue's critical systems. Examples of risks that may affect the operation of Trading Venues include errant algorithms, inadequately or improperly tested changes to participant systems and order entry errors.

Furthermore, many Trading Venue participants facilitate the execution of orders by providing clients with direct electronic access (DEA Clients).[56] These clients may also rely on technology to generate or send orders. As a result, issues or incidents with DEA Clients' technology may adversely impact the Trading Venue's systems and thus market integrity.

Issues with participant systems may impact a Trading Venue's ability to maintain a fair and orderly market. This might necessitate a Trading Venue to introduce microstructure mechanisms (such as pre-trade controls, circuit breakers, volatility parameters and kill switches) and tools to manage these risks and address the issues that arise.

In addition, regulators have introduced requirements or guidelines for Trading Venues or Trading Venue participants. These requirements or guidelines often refer to both microstructure tools and policies and procedures to manage risks to systems.

(a) Tools to manage risks that arise from electronic trading

Most regulators require Trading Venues to take steps to manage the risks potentially posed to them by the electronic systems of their Trading Venue participants. Most regulators do not

[56] As used in this survey, the term "Direct Electronic Access (or DEA) Client" means a client of the intermediary (broker-dealer), who is granted access to the market to transmit orders using the intermediary's mnemonic via *either* access through the intermediary's infrastructure/systems, or access without utilization of the intermediary's infrastructure/systems (so-called "sponsored access").

mandate "standardized/specific controls" across venues for addressing erroneous trades or errant participant systems due to the fact that there is a diverse range of market models operating in each jurisdiction.[57] Nevertheless, regulators have generally required Trading Venues to have their *own* controls.[58] Where mandated, the nature of those controls must be appropriate to the nature, scale and complexity of the activity that takes place on the Trading Venue.

With respect to Trading Venue approaches, most Trading Venues have policies, procedures, and tools that are used to mitigate, detect and address the operational risks associated with electronic trading and there are various approaches to manage the risks posed by the electronic systems of their Trading Venue participants. These include:

- policies and procedures and regular monitoring to ensure market participants comply with the rules of the Trading Venue;
- monitoring of trading in real-time (or near real-time), including the capacity to detect abnormal price movements or trading anomalies;
- monitoring of the Trading Venue's system performance in real-time;
- pre-trade controls (*e.g.*, price and volume controls or filters; order entry controls);
- post-trade controls (*e.g.*, trade cancellation policies, post-trade monitoring of positions/exposure);
- the ability to block, suspend or disconnect a user if required (*e.g.*, kill switches);
- error trade cancellation policies – to cancel, amend or correct a transaction;
- measures to constrain or halt trading in the face of sudden price movements including collars on price movements (*e.g.*, limit-up-limit-down), and volatility measures;
- circuit breakers (single stock and market-wide) to stop trading during unusually volatile trading periods;
- measures to address excessive message traffic; and
- measures to constrain the number or frequency of messages received from any given participant (*e.g.*, throttling).

Trading Venue participants also have a role in managing risks to trading arising from access by their systems to Trading Venues. Many Trading Venue participants use pre-trade risk and other controls to prevent erroneous orders. Specific limits that are used relate to: order volume, price per security, credit, notional value of order, order value, capital, position checks, price deviation thresholds, and regulatory integrity checks (for example, checking for compliance with order protection rules). Many Trading Venue participants automatically reject an order that breaches these limits. Sometimes they use soft limits whereby a warning indicating that a hard limit is being approached is sent to a trader who can help ensure that appropriate action is taken to prevent an order from being rejected because of crossing a hard limit.

---

[57] For example, Ireland, Italy, Romania and the UK.

[58] *See* IOSCO Report: Policies on Error Trades (Oct. 2005), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD208.pdf.

Should an incident occur, most Trading Venue participants report having the capability to track orders, including modifications, cancellations and identification of trading strategies and the use of trading algorithms.

(b) Managing risks due to new, and changes to Trading Venue participant systems

Potential risk to the Trading Venue is introduced whenever Trading Venue participants make changes to their systems that access Trading Venue's systems, particularly when such systems have not been properly developed and tested. In recognizing the importance of their systems and the potential impact on the firm and others should something go wrong, market participants often have specific internal procedures or management processes in place to address associated risks. These include testing systems as part of quality assurance, prior to implementation of new systems and before changes to existing systems are implemented. Both regression[59] and non-regression[60]testing may also be undertaken.

To test robustness and availability, many market participants conduct stress testing frequently, with particular emphasis on the creation and addition of scenarios.[61] Most Trading Venue participants also conduct performance and volume tests. In addition, Trading Venue participants reported having monitoring systems/tools to monitor order flow and the use of alerting systems on the capacity and performance of systems, and coordinating testing with Trading Venues.

(c) Managing risks due to DEA Client order flow

Where there is significant order flow being sent electronically from a DEA Client (for example, using an algorithm) through a Trading Venue participant, the same risks as those raised by Trading Venue participant systems arise. Errors that are caused by the incorrect deployment of new, or changes to, the DEA client systems, or a lack of monitoring of the performance of these systems may impact trading on the Trading Venue.

In 2010, IOSCO issued a report entitled *Principles for Direct Electronic Access to* Markets.[62] In that report, IOSCO recognized the need for Trading Venue participants (*i.e.* intermediaries) to

---

59 Regression testing is a type of software testing that seeks to uncover new software bugs, or *regressions*, in existing functional and non-functional areas of a system after changes such as enhancements, patches or configuration changes, have been made to them. The intent of regression testing is to ensure that system changes have not introduced new faults. One of the main reasons for regression testing is to determine whether a change in one part of the software affects other parts of the software.

60 Non-regression testing (NRT) is an approach to software testing. The purpose of non-regression testing is to verify whether, after introducing or updating a given software application, the change has had the intended effect. Contrast with regression testing which aims to show that the change has not had an unintended effect on the software.

61 Stress test scenarios include: (1) doubling the number of orders and executions compared to a regular trading day; (2) doubling the peak volumes observed for a period; (3) tripling the current maximums experienced in current production; (4) testing volume of 130% of volume traded the previous two years; and (5) testing ten times the current trading volume when developing new algorithms and systems.

62 Annex 3 sets forth the principles of that report.

introduce the appropriate controls to manage the risks associated with electronic trading and DEA access. To that end, IOSCO included a principle that stated: *Intermediaries (including clearing firms) should have adequate operational and technical capabilities to manage appropriately the risks posed by DEA.*

As discussed, some jurisdictions require pre-trade controls to be implemented on all order flow entering Trading Venues from Trading Venue participants, including flow from DEA Clients. These controls may include thresholds that identify when there are systems issues impacting order flow (for example, algorithm loops). Trading Venue participants generally apply these types of controls to monitor and manage the order flow coming from DEA clients.

There is no common approach amongst regulators with regard to ensuring the integrity of DEA Clients' systems.[63] Some Trading Venue participants appear to acknowledge the need for testing of the DEA Clients' systems, acquiring descriptions of a DEA Client's algorithms (with potential compliance checks), and DEA Client testing of algorithms and pre-trade controls (in coordination with the DEA provider). Indeed, a DEA Client may conduct testing in response to a request by the Trading Venue participant, yet this does not appear to be done systematically or to be a widespread practice.

Many intermediaries responding to the IOSCO survey who have DEA Clients stated that they do not test their DEA Clients' systems or request information from them regarding their algorithms and trading technology. With regard to the first time that a DEA Client uses the Trading Venue participant's systems infrastructure, a few responding intermediaries conduct "some" testing before granting access to their new DEA Clients, *e.g.*, connectivity testing, algo-testing and pre-trade risk checks. Occasionally, systems compatibility is tested and/or DEA providers or external auditors must certify the DEA Client's systems.

Most Trading Venue participants confirm that tests are run after any significant change in a DEA Client's systems, although this may only be done if it is made aware of such a major change and may only consist of an "attestation" from the DEA Client of annual testing. Some Trading Venue participants expressed the view that it is important for their DEA Clients to keep evidence of their tests, while at the same time maintaining that it is the responsibility of the client to conduct testing, rather than the Trading Venue participant's.

2. Risks posed by cyber-attacks

Cyber-attacks on a Trading Venue's critical systems may impact the resiliency, integrity and robustness of the Trading Venue.[64] A cyber-attack refers, in general terms, to an attack on the confidentiality, integrity and accessibility of an entity's online/computer presence or networks.

---

63 In Canada, intermediaries with market access are required to understand the algorithms of their clients and ensure that the algorithms are appropriately tested. See NI 23-103. *See also* SEC Rule 15c3-5, promulgated under the Securities Exchange Act of 1934.

64 See footnote 18.http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

Such attacks can involve data theft, destruction or manipulation; identity theft; monetary theft; disruption of IT services; and, in some cases, cyber-espionage and cyber-terrorism.[65] A breach of cyber-security on a Trading Venue or a Trading Venue participant has the potential to disrupt:

- the ability of a participant to send orders to a Trading Venue;
- the ability of a Trading Venue to execute orders or execute them properly, which can compromise fair and orderly markets; and
- investor confidence.

(a) Regulatory requirements relating to cyber-security of Trading Venues

A number of regulators have publicly expressed support of specific requirements on Trading Venues to ensure that they take the steps necessary to protect themselves against potential cyber-security risks. Existing requirements that are relevant to cyber-security include those relating to system access control, physical and electronic security of critical systems, authentication, transaction authorization, data integrity, system activity logging, audit trail and security event tracking. In addition to these requirements, regulators generally cover cyber-security risks related to Trading Venues activities through their on-going oversight program, including through the assessment of a Trading Venue's policies, procedures and BCP plan, or via scrutiny of the independent systems review conducted by the Trading Venue and filed with the regulator.[66] There may also be reporting requirements in the case of a cyber-security breach or threat, or where there is a relevant systems failure or a serious risk of such a failure.[67]

Although some jurisdictions have high-level regulations relevant to cyber-security (*e.g.*, a Trading Venue must have a "security process in place"), others have just provided guidance. For example, many have adopted general guidelines, including those set forth by supranational organizations.[68]

---

65 Ibid.

66 Australia, Canada, Ireland, Japan, Mexico, Turkey, Malaysia, Singapore, US (CFTC), and SEC) and India).

67 As an example, the U.S. CFTC requires designated contract markets to notify the CFTC promptly of all cyber-security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity." In Canada, regulation applicable to systems that support order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing covers cyber-security risks and includes a reporting requirement in case of material systems failure, malfunction or delay. However, more detailed requirements respecting security threats controls and security breaches notification have been proposed. Another example is the Japan Financial Services Agency that requires detailed report on system failures. *See also* US SEC Regulation SCI, Rule 1002.

68 ESMA published a guideline addressing this topic that provides for trading platforms to have procedures and arrangements for physical and electronic security designed to protect their electronic trading systems from misuse or unauthorized access and to ensure the integrity of the data that is part of or passes through the systems. The Monetary Authority of Singapore published guidance that covers cyber-security risks. In particular, financial institutions in Singapore are expected to establish sound technology risk management and security practices to ensure the confidentiality, integrity and availability of their data and systems. The guidance emphasizes that Information Technology (IT) is vulnerable to various forms of cyber-attacks and warns that the frequency and malignancy of attacks are increasing. The guidance also emphasizes that it is imperative that financial institutions implement security solutions at the data, application, database,

(b) Trading Venues and cyber-security

Effective governance is critically important to control cyber-security risks and respond effectively to cyber-attacks and Trading Venues use a variety of measures to do this. Typically, a senior manager, such as a Chief Information Security Officer or equivalent, is responsible for operationalizing the security framework. A committee and/or the board of directors as well as operation, risk and compliance departments may also be involved in ensuring steps are taken with respect to cyber-security. Almost all of the Trading Venues have implemented notification or reporting frameworks to senior management in accordance with internal rules in order to respond quickly to a security breach or an incident that threatens critical systems. Most Trading Venues also stated that they have mechanisms in place to provide details to regulators regarding possible or actual breaches of security.

In addition, Trading Venues have taken steps to educate staff regarding the risk of opening emails or attachments from unknown sources. These emails or attachments may contain viruses or programs that can negatively impact the Trading Venue's systems.

There are a number of safeguards that Trading Venues have taken to protect against cyber-attacks. Some of the Trading Venues conduct on a periodic basis penetration and vulnerability tests to ascertain the effectiveness of their security systems.

Trading Venues have also taken steps to safeguard data storage and integrity by introducing data backup through secondary data centers and/or off-site storage. They control access through encryption, firewalls, using password and/or electronic keys and network segregation. In fact, Trading Venues indicated that data tends to be segregated, and access to the data is strictly controlled and audited. Moreover, Trading Venues may control and monitor access using authentication mechanisms to secure data in accordance with a Trading Venue's business and technological requirements and, in some cases, audit trails are generated by the application systems for detecting illegal access. In addition, Trading Venues often separate duties between personnel that manage access to critical systems and personnel on the team responsible for operating the systems.

To ensure the effectiveness of monitoring and surveillance of these mechanisms to detect cyber threats and suspicious system/network activities, some Trading Venues have adopted mechanisms such as intrusion prevention and detection systems and firewalls. Systems that detect, analyze and alter possible cyber-security threats and suspend network activity allow the Trading Venue to monitor for malware, suspicious code, vulnerabilities and malicious internal activity.

---

operating systems and network layers to address and contain these threats adequately. The guidelines further provides for the implementation of appropriate measures to minimize exposure to other forms of cyber-attacks such as the so-called "middleman attack," which is more commonly known as "a man-in-the-middle attack" (MITMA), "man-in-the browser attack" or "man-in-the application attack."

(c) Trading Venue participants and cyber-security

Another potential threat to Trading Venues is the possibility that there is unauthorized access to the Trading Venue systems through a Trading Venue participant's system. As a result, it is important to understand what steps intermediaries take to protect themselves from cyber-security breaches. In this regard, IOSCO notes that most of its members require the intermediaries subject to their jurisdiction to have a BCP and to manage business risks appropriately, which includes cyber risks.

The vast majority of surveyed intermediaries stated that they have in place arrangements to address the risks posed by potential cyber-attacks. Firms often have an organizationally independent entity and/or person in the firm that is in charge of the global information security policy, including its implementation and monitoring.

One important tool utilized by the majority of respondents is some form of separation from the World Wide Web in order to reduce a potential intrusion from outside the firm. If the Internet is used for access, enhanced safety is achieved through encryption or the use of virtual private networks.

Another tool used by intermediaries is regular penetration testing**.** This might be performed with a focus on external gateways or in a more broad fashion involving a firm's own experts who are knowledgeable about hacker techniques. Such specialized tests or procedures are often outsourced to an external expert service provider.

Finally, almost all intermediaries use IT-tools, which are designed to prevent unauthorized access, such as firewalls, anti-virus/malware software and similar mechanisms. These measures to prevent penetration of one's network are usually complemented by monitoring systems that are designed to detect security breaches.

3. Sound practices relating to external risks to a Trading Venue's systems

In addition to the sound practices discussed above, there are a number of sound practices that a Trading Venue should consider in order to manage external risks to its critical systems. As noted above, however, it is within an individual Trading Venue's discretion to determine which may be appropriate for them. Specifically, a Trading Venue 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 halt trading 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.

F. HOW TO PLAN FOR DISRUPTIONS: BUSINESS CONTINUITY PLANS

One of the key steps to address the risks associated with technology is the development of a BCP, which incorporates significant components of operational risk management, and 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 the BCP is to minimize the operational, financial, legal, reputational and other potential material consequences arising from a disruption. Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which affords financial industry participants and regulatory authorities greater flexibility to address a broad range of disruptions. At the same time, however, organizations cannot ignore the nature of the risk to which they are exposed.

Principle 2 of the Joint Forum Report stated that "[f]inancial industry participants [a term that includes Trading Venues] should incorporate the risk of a major operational disruption into their approaches to business continuity management." The Joint Forum defines a "*major operational disruption*" as "[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.*[69]

[69] The report also notes that "*[m]ajor operational disruptions* 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*. 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. Events whose impact is most significant are referred to as "extreme events". They involve one or more of the following: the destruction of, or severe damage to,

Consistent with the Joint Forum Report, a Trading Venue's recovery and business continuity tools and plans must consider the operational risks it faces that may lead to trading or major operational disruption due to, for example: (1) trading disruptions caused by technological issues and/or systems malfunctions; (2) IT security disruptions, such as viruses, and/or cyber-attacks; or (3) market-wide disruptions caused by exceptional events, such as natural disasters or acts of terrorism. The key components of the BCP and the regulatory requirements relating to them are discussed below.

1. Regulatory requirements relating to the BCP

Regulators have recognized the importance of robust Trading Venue BCPs. Many regulators require a Trading Venue to have an appropriate BCP[70] and often require a Trading Venue to provide them with a copy or description of, or rules relating to the BCP. Regulators may also have the authority to assess a Trading Venue's BCP and will consider several factors as part of the assessment, including:

- the scope and nature of services that are considered to be critical;
- whether any service is outsourced;
- governance and escalation procedures;
- internal and external communication arrangements;
- compliance with regulatory requirements for BCPs for policies and procedures that seek to ensure uninterrupted provision of key services.[71]

---

physical infrastructure and facilities; the loss or inaccessibility of personnel; and, restricted access to the affected area." Joint Forum Report at 3.

[70] For instance, Canada, France, Hong Kong, India, Italy, Japan, Malaysia, Romania, Singapore, Spain, U.S. (CFTC and SEC). In Europe, Trading Venues are required to comply with ESMA Guidelines on Systems and Controls in an Automated Trading Environment for Trading Platforms, Investment Firms and Competent Authorities (ESMA Guidelines). These ESMA Guidelines cover resilience, business continuity and systems testing among other areas and were cited by certain regulators as relevant to the ongoing supervision of BCPs. South Africa and Australia require a report prepared by a third party to confirm that a Trading Venue's BCP has been implemented. ASIC in Australia requires an attestation that the BCP has been successfully tested prior to granting a license to the Trading Venue. South African regulators require confirmation that the Trading Venue has a BCP, that necessary service level agreements with third parties are in place and that adequate disaster recovery hardware and related facilities are located off-site. The US CFTC requires as a condition for both initially obtaining and thereafter maintaining designation that a contract market establish and maintain emergency procedures, backup facilities and a plan for disaster recovery that allow for the timely recovery and resumption of operations. In the US, the SEC adopted Regulation SCI, which requires SCI entities to establish business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption.

[71] Australia, Brazil, Canada, France, Germany, Hong Kong, India, Malaysia, Mexico, Netherlands, Romania consider all of the factors while others (Italy, Japan, Singapore) consider a subset of these factors when reviewing a BCP. Regulators in Hong Kong and Spain additionally look for sufficient training to be provided to staff related to BCP procedures. In 2003, the SEC issued a policy statement setting forth its view that SROs (which include exchanges) and electronic communication networks (ECNs) should apply certain basic principles in their business continuity planning. *See* Securities Exchange Act Release No. 48545 (Sept. 25, 2003), 68 FR 56656 (Oct. 1, 2003) (Policy Statement: Business Continuity Planning for

2. Trading Venue BCPs

Trading Venues have taken steps to create, manage, update and test their BCPs. BCPs provide for different scenarios, governance, back-up or redundancy, minimum service levels, communications protocols and regular testing and review.

(a) Scenarios

Trading Venues that adopt BCPs create a list of scenarios that could trigger their BCP. In doing so, they focus on internal risks and external risks. The range of adverse scenarios varies widely from one Trading Venue to another. Some approaches focus on the cause of the disruption while others on the impact. Some of the main scenarios contemplated by Trading Venues include:

- system and network failures
- data dissemination failures
- pandemics
- natural disasters
- power failures
- cyber-attack
- communication disruptions
- loss of key staff
- loss of regular access to premises.

Each of these scenarios may lead to a different degree of disruption, which the BCP may take into account when outlining escalation procedures and incident management policies and procedures. Trading Venues use a variety of approaches in assessing the impact of a scenario on critical systems and activities; these are based on an analysis of the capability and capacity to carry out the provision of services to a client without major degradation of the service. The assessment of 'major degradation' is subjective and there are few official benchmarks that exist to make this kind of assessment, such as ISO certifications.[72]

Trading Markets) (''2003 Policy Statement on Business Continuity Planning for Trading Markets''), http://www.gpo.gov/fdsys/pkg/FR-2003-10-01/pdf/03-24863.pdf. In addition to what is stated in the previous footnote, Regulation SCI also requires annual BCP/DRP plan testing with members or participants, as well as industry- or sector-wide testing of such plans. 17 CFR 242.1001, 1004. US CFTC rule 38.1051 requires a contract market's disaster recovery plans and resources to allow resumption of the market's ongoing responsibilities, which include, without limitation, the following performance objectives: order processing and trade matching; transmission of matched orders to a designated clearing organization for clearing; price reporting; market surveillance; and maintenance of a comprehensive audit trail; and resumption of trading and clearing of the market's products the next business day following the disruption. The US CFTC also requires that testing should be conducted by qualified, independent contractors or employees of the market, but should not be persons responsible for development or operation of the systems or capabilities being tested.

[72] For example, ISO22301:2012(business continuity) and BS 25999-2:2007 (business continuity management).

(b) Governance

Clarity around the governance of BCPs and their implementation is important. Many Trading Venues have a dedicated officer (*e.g.*, Chief Risk Officer (CRO) or Chief Operating Officer (COO)), separate from those responsible for IT matters, who is responsible for the development and ongoing review (updating) of the BCP. Alternatively, Trading Venues may have risk management committees responsible for the approval of a BCP and related procedures. These committees may be made up of senior management and are responsible for leading the business impact assessment to identify critical processes, determine recovery time and recovery point objectives (see sub-section (d), below), reviewing and certifying BCP/DRP arrangements and for coordinating any response to any incident that arises that triggers the plans.

Trading Venues will also often have "incident/crisis management" teams that are responsible for strategic decisions and operations when BCPs are triggered by an incident/crisis. CEO/COO/Head of IT as well as top managers of the business units are usually part of the incident/crisis management team.

Escalation procedures included as part of the BCP often depend on the severity of the incident, while for others it will vary depending on the business unit where the incident originated. In most cases, the person in charge of the crisis management team raises the issue with senior management and the Board. The escalation procedures are similar across Trading Venues and include event identification, obtaining information, impact analysis, and possible activation of BCP, depending on the severity of an event.

(c) Redundancy

All surveyed Trading Venues, as part of their BCPs, have a back-up operating site. In addition, Trading Venues' server environments, critical hardware and software components are usually duplicated across the primary and backup data centers. If the primary site is down, operations should be able to switch to the contingency site in order to continue to carry on business.

Many Trading Venues appear to require that the back-up site be "hot" (*i.e.* the secondary core should be in an identical state to the primary data center, meaning all critical business data is accessible). BCPs commonly require independent electricity sources and climate controlled environments. The time anticipated by BCPs that will be needed to move the staff to the back-up site ranges from 15 minutes to 4 hours.

All surveyed Trading Venues stated that, in considering the acceptable distance between the primary and secondary, operating sites, the Trading Venue should look at the risk profile between each location instead of a distance measurement, to ensure that each operating site is, for example, on a different power, gas, and water and transportation grid. In other words, the minimum distance will depend on the assessment of the geographical area risks (seismic, natural catastrophes, extreme weather conditions, political instability risks). Therefore, the decision on the location of the data center is usually decided with comprehensive consideration given to

factors including the facility's capabilities, the low probability of being affected at the same time as the primary site when a risk materializes, and the ease of sending staff to the backup site.[73]

In developing their BCPs, most surveyed Trading Venues do not consider whether securities traded on their own platform are also traded at other venues, with some exceptions.[74]Among other reasons, they cite the differences between Trading Venues' technological systems, the range of securities or asset classes traded within a given Trading Venue, and the fact that certain venues trade in only one specific asset class (e.g., stocks, bonds, etc.) as reasons. In addition, for those Trading Venues that trade more than one type of security, their BCPs generally do not anticipate different actions for continued trading in specific types of securities.[75]

(d) Minimum service level of the critical functions

All Trading Venue BCPs appear to identify, for each of the critical services/activities and systems, the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for the services/activities and systems operated.[76] RTO and RPO are usually defined by Trading Venues through a business impact analysis process in which each critical system is assessed individually and RTO/RPO identified and included in the BCP. The business impact analysis is usually reviewed on a yearly basis. In case of outsourcing, RTO/RPO are in most of the cases included in the SLA.

All Trading Venues' BCPs anticipate a minimum service level of the critical functions and an expected timing of the completion of the full recovery of the processes. In terms of the expected

---

73 Survey results indicate that the physical distance between the sites is around 10/15 km for most of the Trading Venues, with a range of 5-1000 km. Specific consideration is given to separation of utility supplies (power substations, communications paths, water mains, telephone exchanges, etc.) as well as the ability to operate from multiple locations that can change and adapt to changing conditions and the identification of key-essential staff to keep business in operation along with the means to allow them to operate on a remote basis.

74 For example, a Trading Venue in Australia considers other market operators and they are explicitly captured in the incident management team procedures and communications check lists, with key contact details readily available. In Canada, an alternative trading system (ATS) considers other Trading Venues due to the multi-market framework since all the products they trade are listed on multiple market places; consequently, if a major disruption occurs, they are able to route the order flow to other available Trading Venues. Another Trading Venue in Canada has a process whereby a marketplace/ATS/Participating organization can declare self-help in the event they cannot access a Trading Venue; the process is undertaken in conjunction with the securities regulator.

75 However, an Italian Trading Venue stated that it considers different "recovery times of operation" for different securities, based on recommendation by the Central Bank of Italy. In addition, Japan has a comprehensive contingency plan for individual products and Korea recognizes that they have common and specific provisions for different securities. In several jurisdictions, big groups operating several trading platforms have one overall business continuity plan due to different securities that are traded in different platforms, but specific recovery plans may differ in content.

76 The RTO is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. The RPO is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

timing of the completion of the full recovery of the processes, most Trading Venues' BCPs require the venue to be able to recover within 2 to 4 hours. The RPO is usually less than 30 minutes and where data is synchronously mirrored in real-time to backup systems, it is close to zero.

Data integrity is critical in order to recover from a disruption to the trading environment. Therefore most of the Trading Venues' BCP require that all necessary steps be taken to ensure that data (both internally and distributed to the participants) is fully consistent before trading can resume. Where data issues arise, Trading Venues decide whether (and when) to resume trading.

(e) Communication

Communication protocols are generally included in the procedures set forth in a Trading Venue's BCP and govern all communications, with regard to both internal and external communications in the event of a major operational disruption. The main factors or key inputs to consider are severity, timing, impact and the parties affected.

Some regulators require Trading Venues to notify them whenever they experience a major operational disruption.[77] In addition, some regulators require a follow-up incident report from the Trading Venue that explains the root cause of the incident and any measures taken by the Trading Venue to address the issue.[78]

In most cases, Trading Venues have a protocol that lists the relevant parties to notify. With regard to internal communications associated with an event that has triggered a BCP, all surveyed Trading Venues have procedures for prompt distribution of information guided by the procedures set forth in an Incident Management Plan or documented BCP. Incident managers must arrange for the proper collection and distribution of relevant information to ensure proper impact assessment and communication of the incident. Some Trading Venues indicate they have call cascades/trees and contacts within the BCP, as well as call-out procedures. Recovery team leaders provide ongoing updates such as business impact and recovery status. All of them use common tools, including corporate email, and landline and mobile phones; two Trading Venues indicated that they have emergency contact systems or automated notification systems that assemble the team at a conference bridge or command center. Communication must take place as soon as possible and as close to real time as possible.

With respect to external communication to the public, senior management is generally involved in communicating a Trading Venue's response to an event that triggers a BCP. Many Trading Venues will disclose publicly the triggering of a BCP on their Web sites and provide updates, as necessary. Most Trading Venues stated that the frequency and content of communication depends on the nature of the crisis or different scenarios. Some protocols specify a frequency for

---

[77] Australia, Canada, ESA (Hessen), Hong Kong, India, Italy, Malaysia, Romania, Singapore, Spain, South Africa and the U.S. SEC and CFTC (*see* Joint Forum definition of a major operational disruption, above).

[78] Australia, Canada, Hong Kong, India, Italy, Malaysia, Singapore, Spain, and U.S.

communications (for example, updates provided once per hour or different frequency for internal, regulatory and public communications).

(f) Recordkeeping

All surveyed Trading Venues have explicit procedures or policies requiring them to maintain a log of actions and decisions taken during a BCP event. In all cases, after the event, they draw up a post-mortem report and include all information not logged during the incident. They analyze all the information logged during the event for root cause determination, review processes, communications recorded during the incident, authorization requests, *etc*. Some Trading Venues also maintain records of relevant e-mails, call logs, systems logs, internal instant messaging conversations and other things.

(g) Testing and periodic review

Many regulators require regular assessments or testing of the Trading Venue's BCP.[79] Of those, some also require the Trading Venue to continuously maintain or update BCPs,[80] while others require changes to BCPs to be filed with them for approval.[81] Finally, some (but not all) jurisdictions require Trading Venues to participate in periodic, synchronized BCP testing (*i.e.*, industry-wide tests). However, interoperability arrangements with other Trading Venues and interaction with other financial market infrastructures is not always part of such tests. In some cases, Trading Venue participants are invited (or even required) to participate in periodic tests.

Key components of BCP arrangements (such as access to site and system, availability and relocation of staff, governance, communication, backup systems in a secondary site and recovery procedures) are generally reviewed and updated periodically. Trading Venues indicate that current practice is to do this review on an annual basis and, in some cases, twice a year or even more frequently. Typically, any incident that triggers a BCP necessitates a review of the BCP.[82] Most Trading Venues agree that any deficiencies identified in testing need to be remedied

---

79 Australia, Brazil, Canada France, ESA (Hessen), Hong Kong, India, Malaysia, Mexico, Netherlands, Singapore, Spain and U.S. (CFTC and SEC)

80 Australia, Brazil, Canada, France, India, Italy, Malaysia, Mexico, Netherlands, Romania, Singapore and Spain.

81 Germany. In South Africa, the Trading Venue must confirm that the plans are reviewed for adequacy and updated as necessary. In the U.S., the U.S. SEC can review a Trading Venue's BCP as part of an inspection or examination and request additional information about it. The US CFTC reviews these plans both as a matter of initial designation and thereafter as a matter of ongoing compliance reviews.

82 We note, however, that few of the Trading Venues surveyed by IOSCO indicated that they had faced in the recent past faced major operational disruptions. Indeed, only a few have activated their BCP. The events that led to the triggering of the BCP included (1) a power outage, (2) the precautionary closing of a building because of a communicable disease, (3) natural catastrophe or weather related event, and (4) an internal network disruption. In all of these situations, the Trading Venues indicated that their BCPs functioned as expected.

swiftly. Some Trading Venues also note that they participate in industry-wide testing every two years, and in some cases, annually.

Other respondents to IOSCO's survey indicate their reviews are aligned with industry best practice or guidelines from their regulator. Senior officers are often responsible for reviewing the BCP (such as the Chief Risk Officer or the Group Head of Business Resilience), although it may also be conducted by an internal department (such as IT strategy/ IT security/risk management) and reviewed by internal audit. In some cases, there is also a periodic or occasional review by national regulators or independent external auditors.

(h) BCP and outsourced services

With only a few exceptions, all of the surveyed Trading Venues explicitly take into account the possibility that firms supplying outsourced services will become unavailable. Approaches differ in the way BCP account for this possibility and the potential impact on the market and on external customers.

The obligations usually covered in relevant SLAs include a requirement for the continuity of services, alternatives/workarounds in case of disruption of the service, and the maximum time that the service provider may take to respond to issues. It may also include provisions relating to RTO and RPO, reporting obligations in case of incidents, key contacts for each party, escalation procedures, and compensation (penalties/remedies) for non-compliance with service levels.

Generally, little information is made available to Trading Venues in relation to the supplying firm's business continuity or disaster recovery arrangements of the entity providing the service/activity. In a few cases, the Trading Venue has access to the BCP information document (or a part of it) of the service provider. In addition, the supplying firm may simply provide the Trading Venue with a written statement in which the firm indicates that it has an active BCP that is suitable for their business.

As a result, few Trading Venues are able to perform a specific "quality" assessment of the service provider. Those that do indicated that the assessment is made through participation in joint BCP exercises. The results from testing, either directly or through sector/industry testing, along with a proven history of providing uninterrupted services, help to validate the quality of the supplying firm's BCP. In a few cases, auditors or Trading Venue examiners will (through regular testing and/or periodic reviews) assess the BCP's quality and compliance with regulatory requirements.

(i) BCP and intermediaries

In most jurisdictions, Trading Venues do not require participants to have a BCP; however, some Trading Venues highly recommend that their participants have a BCP in place. Where Trading Venues require participants to have BCPs, it is usually set forth in regulations or the Trading Venue's own rules. Sometimes, the statutory regulator or self-regulatory organization requires Trading Venue participants to have a BCP.

3. Recommendation and Sound Practices

Recommendation 2 to Regulators

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

This recommendation expresses more directly and clearly the underlying sentiment communicated in the Joint Forum Report that a Trading Venue (and other financial market participants) should be required to have a BCP. This is also consistent with current requirements in most IOSCO member jurisdictions.

The need to require financial market participants to have BCPs was indirectly implied in the Joint Forum Report through the principle that stated that financial industry participants (a term that includes Trading Venues) should have effective and comprehensive *approaches* to business continuity management (a term that includes a BCP).[83] The principles also stated that 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 and that they should also *expect* financial industry participants to develop and implement effective business continuity management that is updated on an ongoing basis.[84]

Sound Practices for Trading Venues

In reviewing the practices of the Trading Venues, IOSCO has identified a number of sound practices relating to BCPs.[85] Trading Venues should[86] consider these sound practices whenever

---

83 [Principle 1 of the Joint Forum Report, see Annex 1.

84 [Principle 7 of the Joint Forum Report, see Annex 1.

85 These sound practices should be read in connection with the Joint Forum's Principle 1, which states that an organization's board of directors and senior management are collectively responsible for the organization's business continuity and that they are responsible for managing its business continuity effectively and for developing and endorsing appropriate policies to promote resilience to, and continuity in the event of, operational disruptions. According to the Joint Forum, the board and senior management should create and promote an organizational culture that places a high priority on business continuity, which should be reinforced through the provision of sufficient financial and human resources to implement and support the organization's approach to business continuity management. The Joint Forum Report also states that the organization should implement a framework for reporting to the board and senior management on matters related to business continuity, including implementation status, incident reports, testing results and related action plans for strengthening an organization's resilience or ability to recover specific operations. An organization's business continuity management should be subject to review by an independent party, such as internal or external audit, and significant findings should be brought to the attention of the board and senior management on a timely basis. Further, that senior management should recognize that they may need to re-align priorities and resources during a disruption in order to expedite recovery and respond decisively. It is important that a locus of responsibility for managing business continuity during a disruption is established, such as a crisis management team with appropriate senior management membership. In addition, senior management should be involved in communicating the organization's response, commensurate with the severity of the disruption.

developing a BCP. They are intended to allow for a wide range of application and adaptation in different jurisdictions, subject to local regulatory requirements. Nevertheless, it is within an individual Trading Venue's discretion to determine which may be appropriate for them.

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.[87]

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.[88]

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

---

86 National regulators may require all (or some) Trading Venues subject to their jurisdiction to comply with one or more of these practices. Nothing in this section should be interpreted to suggest that these regulators should change such requirements.

87 This is very similar to Joint Forum Principle 2, which states: "*financial industry participants…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.*"

88 We note that paragraph 24 of the Joint Forum Report states that the Board and senior management "should recognize that outsourcing a business operation does not transfer the associated *business continuity management* responsibilities to the service provider."

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.

G. CONCLUSION

This report 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.

Annex 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 organization's board of directors and senior management are collectively responsible for the organization'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 organizations 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.

Annex 2

IOSCO Report: *Principles for Outsourcing by Markets*

On July 13, 2009, IOSCO published a final report *Principles for Outsourcing by Markets* (Outsourcing Principles) containing a set of principles designed to assist market operators[89] i.e. exchanges, and market authorities when considering outsourcing arrangements.

The Outsourcing Principles set out the factors that market operators should consider when deciding whether, and to whom, to outsource processes, services or functions, and are also designed to assist market authorities in their oversight of these arrangements. These principles were developed following an earlier IOSCO report on *Regulatory Issues Arising from Exchange Evolution* which identified outsourcing amongst regulatory issues causing concern arising from the new business model of exchanges In particular the report focused on the issues that could arise once exchanges began to consider outsourcing activities relating to regulatory and key operational functions.

Outsourcing can bring substantial benefits for markets particularly through the lowering of costs whilst allowing access to a high level of expertise and the latest technology. However, it also raises a number of issues that may impact on the effectiveness and integrity of markets related to their ability to manage risks and monitor compliance with regulatory requirements. Outsourcing thus poses a number of important challenges to both markets and market authorities and these principles are designed to address those concerns.[90]

Principles for Outsourcing by Markets

The following areas and related principles have been identified as requiring consideration when a market outsources any of its processes, services or functions:

1. Due diligence in selecting the service provider and in monitoring the service provider's performance

Principle: An outsourcing market should conduct suitable due diligence processes in selecting an appropriate third party service provider and in monitoring its ongoing performance.

The outsourcing market should also take appropriate steps to identify any conflicts of interest between the outsourcing market and the service provider (including affiliated entities and sub-contractors) and ensure that policies and procedures are in place to mitigate and manage any potential conflicts of interest which have been identified or could arise.

---

89 For the purpose of the Outsourcing Report, the term "market¨ referred to exchanges only and does not include Alternative Trading Systems (ATS) or Multilateral Trading Facilities (MTFs).

90 Text taken from the IOSCO press release issued July 13, 2009.

2. The contract with a service provider

Principle: There should be a legally binding written contract between the outsourcing market and each third party service provider, the nature and detail of which should be appropriate to the materiality and nature of the outsourced activity to the ongoing business of the outsourcing market.

3. Business Continuity at the Outsourcing Provider

Principle: The outsourcing market should take appropriate measures to determine that its service providers establish and maintain emergency procedures and a plan for disaster recovery, with periodic testing of backup facilities.

4. Security and Confidentiality of Information

Principle: The outsourcing market should take appropriate measures to determine that procedures are in place to protect the outsourcing market¡¦s proprietary, member-related and potentially market sensitive information and software.

The outsourcing market should take appropriate steps to require that service providers protect confidential information regarding the outsourcing market¡¦s members from intentional or inadvertent disclosure to unauthorized individuals.

5. Termination Procedures

Principle: Outsourcing with third party service providers should include contractual provisions relating to the termination of the contract and appropriate exit strategies.

6. Access to Books and Records, including rights of inspection

Principle: The market authority, the outsourcing market, and its auditors, should have access to the books and records of service providers relating to the outsourced activities and the market authority should be able to obtain promptly, upon request, other information concerning activities that are relevant to regulatory oversight.

This Report complements an existing IOSCO report - Principles on Outsourcing of Financial Services for Market Intermediaries - which establishes a set of principles designed to assist regulated market intermediaries in determining the steps they should take when considering outsourcing activities.

Annex 3

IOSCO Report: *Principles for Direct Electronic Access to Markets*

IOSCO published a Final Report – *Principles for Direct Electronic Access to Markets* (DEA Principles) on May 13, 2010. The report contains principles designed to guide intermediaries, markets and regulators in relation to the areas of pre-conditions for direct electronic access (DEA), information flow and adequate systems and controls. [91]

Principles for Direct Electronic Access to Markets

The DEA Principles set out in the report are based on the recognition that markets, intermediaries and regulators must each play a role in addressing the potential risks posed by DEA. In addition regulators should retain the power to allow or prohibit any form of DEA as well as to establish requirements in the DEA area, including pre-trade controls and risk limits and should also exercise regulatory oversight over the decisions made by clients, intermediaries and exchanges.

1. Pre-Conditions for DEA

Principle 1 Minimum Customer Standards

Intermediaries should require DEA customers to meet minimum standards, including that:

- Each such DEA customer has appropriate financial resources;
- Each such DEA customer has appropriate procedures in place to assure that all relevant persons:
    - Are both familiar, and comply, with the rules of the market; and
    - Have knowledge of and proficiency in the use of the order entry system used by the DEA customer.

Market authorities should have rules in place that require intermediaries to have such minimum customer standards.

Principle 2 Legally Binding Agreement

There should be a recorded, legally binding contract between the intermediary and the DEA customer, the nature and detail of which should be appropriate to the nature of the service provided. Each market should consider whether it is appropriate to have a legally binding contract or other relationship itself and the DEA customer.

Principle 3 Intermediary's Responsibility for Trades

An intermediary retains ultimate responsibility for all orders under its authority, and for compliance of such orders with all regulatory requirements and market rules.

[91] Taken from the IOSCO press release issued on August 13, 2010.

In those jurisdictions where a DEA customer is permitted to sub-delegate its direct access privileges to another party (a sub delegate), the intermediary continues to be ultimately responsible for all orders entered under its authority by the sub delegate and should require the sub-delegatee to meet minimum standards set for DEA customers in general. There should be a recorded, legally binding contract between the DEA customer and the sub-delegatee, the nature and detail of which should be appropriate to the nature of the service provided.

2. Information Flow

Principle 4 Customer Identification

Intermediaries should disclose to market authorities upon request and in a timely manner the identity of their DEA customers in order to facilitate market surveillance. In those jurisdictions where sub-delegation is permitted, the intermediary also has such responsibility to the market authorities with respect to any sub-delegatees.

Principle 5 Pre and Post-Trade Transparency

Markets should provide member firms with access to relevant pre and post-trade information (on a real time basis) to enable these firms to implement appropriate monitoring and risk management controls.

3. Adequate Systems and Controls

Principle 6 Markets

A market should not permit DEA unless there are in place effective systems and controls reasonably designed to enable the management of risk with regard to fair and orderly trading including, in particular, automated pre-trade controls that enable intermediaries to implement appropriate trading limits.

Principle 7 Intermediaries

Intermediaries (including, as appropriate, clearing firms) should use controls, including automated pre-trade controls, which can limit or prevent a DEA customer from placing an order that exceeds a relevant intermediary's existing position or credit limits.

Principle 8 Adequacy of Systems

Intermediaries (including clearing firms) should have adequate operational and technical capabilities to manage appropriately the risks posed by DEA.