Principles for Direct Electronic Access to Markets

Final Report

TECHNICAL COMMITTEE
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR08/10 **AUGUST 2010**

Contents

Chapter 1 Introduction

In February 2009, the Technical Committee of the International Organization of Securities Commissions (IOSCO) published a Consultation Report entitled *Policies on Direct Electronic Access (*Consultation Report*)*.[1] The Consultation Report identified and discussed the benefits, potential risks and concerns that were associated with the use of direct electronic access (DEA) arrangements that permit customers of market members to enter orders into a market's trade matching system for execution.[2] It also addresses issues raised when a non-intermediary such as a hedge fund or proprietary trading group becomes a market member. The Consultation Report is based on surveys of regulators and industry conducted by the relevant Technical Committee Standing Committees on the Regulation of Secondary Markets (TCSC2) and the Regulation of Financial Intermediaries (TCSC3). Although the Technical Committee recognized the market and regulatory benefits associated with the use of electronic execution systems, it also recognized that the increasing use of electronic access raised several regulatory challenges to markets, intermediaries and their regulators.

The Consultation Report identified three key elements to be considered in the promulgation of guidance by IOSCO in the DEA area:

(i) Pre-conditions for DEA
(ii) Information Flow
(iii) Adequate systems and controls

For each of these elements, the Consultation Report identified possible principles providing guidance in the DEA area, and invited comments from industry and the general public on these possible principles or on any other aspect of the Consultation Report. Following the publication of the Consultation Report, the relevant standing committees of IOSCO engaged in the review of this issue, prepared a Feedback Statement (Appendix II), summarizing the comments received during the consultation phase, and provided the Technical Committee's response to the comments, including changes to the proposed principles on DEA.[3]

This Final Report on *Principles for Direct Electronic Access* (Final Report) sets forth principles to guide markets, intermediaries and regulators under the three elements noted above. The principles are premised on the recognition that markets, intermediaries, and regulators each must play a role in addressing the risks of DEA. The Final Report sets forth elements regarding principles pertinent to DEA, including those that address pre-conditions for DEA, information flow, and adequate systems and controls. A key aspect of the principles provide that neither the market nor an intermediary should offer DEA unless adequate pre-trade information is provided, and both regulatory and financial controls,

---

1 *Policies on Direct Electronic Access*, Consultation Report (IOSCO 2009) available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD284.pdf.

2 See Appendix I for definitions used in this report. The trading model of a Customer calling the intermediary or sending an internet order to the intermediary is not considered to be *direct access* for the purposes of this report.

3 The consultation process resulted in 33 responses from North American, Asian and European jurisdictions. Of these responses, 16 were from intermediaries, nine were from trade associations, five were from exchanges, and three were classified as *other*, including a data vendor.

including automated pre-trade controls, are in place to enable intermediaries to implement appropriate risk limits.

In adopting these principles, the Technical Committee continues, consistent with the policy of flexibility that is expressed in the *IOSCO Objectives and Principles of Securities Principles*[4], to respect the right – and responsibility – of firms to determine the specific types of pre-trade controls that should be implemented and the appropriate risk limits that should apply to any client accessing markets through DEA within the parameters set by regulators. 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. The Technical Committee observes in this regard that globally-active exchanges have developed and continue to improve the risk management tools that are offered as part of their DEA systems. In light of these developments, the imposition of any specific quantitative or technological standards would need to be consistently monitored to ensure that they account for such developments.

In general, the arguments raised by respondents with regard to the principles, and in particular with respect to the need to implement automated pre-trade controls, were well thought out and considered carefully by the Technical Committee. In light of these comments, and after its own careful analysis, the Technical Committee concluded that the need for markets and intermediaries to make available and utilize such automated controls rests on the following basic proposition:

> *Whatever level of risk a firm accepts, it must never be infinite. Rather, the risks undertaken must be limited to an appropriate level commensurate with the capital and other financial resources of the firm and the prudent management of both credit risk and any risk to fair and orderly trading. In an automated trading environment, the only controls that can effectively enforce such limits are automated controls.*

To the extent that regulators establish requirements for clients, intermediaries, and exchanges in this area, they should be consistent with this proposition.

---

4 *IOSCO Objectives and Principles of Securities Regulation*, IOSCO Report, April 2008 available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD265.pdf

Chapter 2 Background and Purpose

As the way in which exchanges and other markets operate has evolved, so too has the means of access to these markets.[5] Securities and derivatives exchanges are today overwhelmingly electronic, which has facilitated their operations globally through various forms of communication. Spurred by the increasing demand by DEA Customers[6] for access to global markets, the means to access markets has evolved through continual innovation.

At the inception of the project that led to the drafting of this Final Report, the Technical Committee was confronted by diverse terminology used to describe the specific arrangements of DEA in various jurisdictions and markets (e.g., "direct access," "direct market access," and "sponsored access."). Moreover, even common terms-of-art carried with them different meanings in relation to local market structures. The Consultation Report therefore adopted working definitions for three major DEA pathways: *automated order routing systems* (AORs), *sponsored access* (SA) and *direct access by non-intermediary market-members*, each of which is defined in Appendix 1.

For the purposes of this Report, DEA is defined as the following three major pathways:

Automated Order Routing through Intermediary's Infrastructure (AOR)
This describes an arrangement where an intermediary, who is a market-member, permits its Customers to transmit orders electronically to the intermediary's infrastructure (i.e., system architecture, which may include technical systems and/or connecting systems), where the order is in turn automatically transmitted for execution to a market under the intermediary's market-member ID (mnemonic).

Sponsored Access (SA)
This describes an arrangement where an intermediary, who is a market-member, may permit its Customers to use its member ID (mnemonic) to transmit orders for execution directly to the market without using the intermediary's infrastructure.

Direct Access by Non-Intermediary Market-Members
This describes where a Person, who is not registered as an intermediary, such as a hedge fund or proprietary trading group, becomes a market-member, and in that capacity, in the same way as members that are registered intermediaries, connects directly to the market's trade matching system using its own infrastructure and member ID (mnemonic). Such non-registrant members must enter into clearing arrangements with and become Customers of a clearing member intermediary.

The ability to transmit orders directly to a market in real time gives DEA users greater control over their trading decisions and reduces latency of execution time. Overall, the different means of accessing markets electronically have facilitated the establishment of globally competitive markets, and have greatly benefited market participants and their DEA Customers by permitting them to transact complicated investment and hedging strategies on a global basis in a matter of milliseconds. The use of electronic systems also has regulatory

5 See definitions in Appendix 1.

6 See definitions in Appendix 1.

benefits, such as the generation of electronic audit trail data, and the enhancement of both trade transparency and the ability of markets, intermediaries and other market members to develop and apply automatic risk management controls as well as the ability of regulators to oversee the establishment and use of such controls.

Nonetheless, IOSCO has identified areas of concern where market authorities[7] may determine that guidance is appropriate. For example, DEA has introduced several regulatory challenges to markets, intermediaries and their regulators. Although the nature of the challenges varies depending upon the type of DEA, they include:

- To what extent a user may access markets outside of the infrastructure and/or control of market intermediaries, which challenges intermediaries' traditional risk management approaches and may make rule compliance and monitoring more difficult , particularly with regard to market manipulation and insider dealing;

- The creation of incentives for intermediaries/Customers to gain execution advantages based on the type and geographic location of their connectivity arrangements, which raises potential *fairness* concerns; and

- Facilitating algorithmic trading through automated systems, which raises issues of capacity and the potential need for rationing bandwidth. Indeed, some *black box* trading systems are capable of transmitting several thousand order messages to a market in less than a second.

This Report describes current DEA arrangements, as well as the regulatory approaches of IOSCO member jurisdictions. It also identifies the commonalities and differences in approaches as they relate to the controls imposed by intermediaries on Customers' direct access to the market for purposes of placement of orders and intermediaries' ability to review trades on a pre- or post-execution basis[8]. However, the Final Report does not attempt to describe in technical detail the specific features of the multitude of DEA systems in existence.[9] Indeed, the technical nature of electronic access systems is complex, varied and

---

7 The term *market authority* is used to refer to the authority in a jurisdiction that has statutory or regulatory powers with respect to the exercise of certain regulatory or supervisory functions over a market. The relevant market authority may be a regulatory body, a self-regulatory organization and/or the market itself.

8 Broader issues raised by screen based trading systems (e.g., issues of system integrity and capacity) were addressed previously by the Technical Committee and thus are not the focus of this Report. *See* IOSCO *Principles for the Oversight of Screen-Based Trading Systems*, Report of the Technical Committee of IOSCO, June 1990 (Screen-Based Principles); and *Principles for the Oversight of Screen-Based Trading Systems for Derivative Products-Review and Addition*, Report of the Technical Committee of IOSCO, October 2000, at p. 5, section III, Part 1, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD111.pdf (2000 Report). In the 2000 Report, the Technical Committee adopted four additional principles that encouraged regulatory authorities to develop cooperative arrangements to address risks that arise from cross-border derivatives markets, to share relevant information in an efficient and timely manner, to maintain a transparent framework for regulatory cooperation, and to take into account a jurisdiction's application of the IOSCO Objectives and Principles of Securities Regulation. *See also*, *Policies on Error Trades*, Report of the Technical Committee, of IOSCO, October 2005, available at http://www.iosco.org/library//pubdocs/pdf/IOSCOPDF207.pdf.

9 In general, the basic technical variations in electronic access range from the *restricted* model of a market providing dedicated communication lines to the trading system as well as all trading software

constantly changing. It is hoped, however, that publication of this report will facilitate a better understanding of the different ways that direct access is regulated and how markets address the relevant issues.

This Final Report identifies and discusses the benefits, potential risks and concerns that are associated with the use of DEA arrangements that permit Customers of intermediaries to enter orders directly into a market's trade matching system for execution. It also discusses DEA by non registered intermediaries in their market member capacity. The Report recognizes that the latter category may not always raise the same issues when compared to AOR or SA. Nonetheless, as noted later in the report, credit risk is a key risk raised by DEA arrangements and a market member who is not a clearing firm poses potentially substantial risk to its clearing firm and the market. It also evaluates the information obtained from markets, intermediaries, and market authorities, both in response to written questionnaires and presentations as well as the request for comment on the Consultation Report.

---

and hardware, to more *open access* models where the market permits access through a combination of means, such as dedicated lines and internet, and allows connections using proprietary market software and hardware, proprietary brokerage software and hardware, third-party vendor software and hardware solutions. In this regard, the responses indicate that most markets generally do not restrict the type of end-user technology. In all cases, each market requires that any direct connections to its trading system meet such market's standards.

Chapter 3 Description of DEA Arrangements

A. Qualifications of DEA Customers and non-Intermediary Market-Members

Market-members who are intermediaries have discretion over which of their clients are given direct market access, provided such DEA Customers meet certain terms and conditions outlined below, which are typically set out in written contractual agreements. Intermediaries generally use a vetting process to determine on a case by case basis which of their clients will be permitted to have DEA. A key element of this vetting process is an analysis of the entire risk profile of the potential DEA Customer, particularly with regard to sponsored access. The client's internal systems of monitoring their own risk are closely reviewed by the intermediary, including whether the client has adequate systems and controls to monitor orders and trades on a real-time basis. In addition, intermediaries report that they review closely some or all of the following factors before granting DEA to their clients:

- Familiarity with market rules;
- Degree of financial experience;
- Prior sanctions for improper trading activity;
- Proven track record of responsible trading and supervisory oversight;
- Ability to meet appropriate credit and risk guidelines; and
- Proposed trading strategy and associated volumes.

In many jurisdictions, intermediaries only permit direct market access to clients that are financial institutions, such as broker/dealers, asset managers, banks, introducing brokers, or other types of entities that are supervised or regulated as a financial institution within the jurisdiction. But even where an intermediary permits non-financial institutions to have DEA, the intermediary generally requires a certain minimum level of customer sophistication.

Some markets permit sub-delegation of a Customer's DEA access to another party, i.e. where a DEA Customer is permitted to delegate its access privileges directly to one or more of its own clients. This is used primarily to accommodate structures of the market-member whose affiliates have DEA Customers outside of the jurisdiction. There are rarely any specific market rules to regulate such sub-delegation.

With respect to the access/membership requirements of non-intermediary market members trading only for own account two broad types of requirements for access to the market generally apply. As for all members, these include (i) qualifications of key individuals such as requisite training or competency and *fit and proper* standards; and (ii) structure, management and resources of the potential member. This latter category generally includes: adequacy of internal controls financial resources, technical systems and operational controls; certification of system requirements; and integrity of order routing systems.

B. Identification of DEA Orders

Markets assign each market-member a mnemonic (identifier or *designated code*); and users must input a username and password to access the market trading system. However, most markets' electronic systems do not identify through the market member's IP address or mnemonic the specific Customers of market-members using AOR or SA, i.e., their systems do not support sub-user identifiers or passwords.

Chapter 4 Market Integrity, Risk Management and Other Concerns Associated with DEA

DEA presents various risks to markets and intermediaries that could impact market integrity, including the ability of the market to maintain fair and orderly trading. Trading and credit risks are also key concerns raised by DEA arrangements. Trading risk can generally be described as the risk to an intermediary regarding compliance with market rules applicable to orders sent to the market and executed on behalf of its clients. As for DEA Customers, trading risk arises irrespective of whether this is done through AOR or SA. This type of risk would be less pronounced for the intermediary who simply clears for a Customer who is a member of the market and is subject to the market's rules.

On the other hand, credit risk refers to the risk arising from the fact that an intermediary is normally financially responsible for the trades of a Customer, and which exists for both clearing and non-clearing members, even though the clearing firm may bear the most pronounced risk as it bears ultimate financial responsibility for a trade (although the non-clearing intermediary is financially responsible to the clearing member).

A. Compliance with Market Rules

All markets that allow their members to offer clients DEA by way of AOR or SA indicated that market-members who are intermediaries remain fully responsible for the orders entered by their DEA Customer. For all markets that allow DEA, the market-member who is an intermediary is thus subject to the market disciplinary procedures whether orders are entered by the member or *through* the member.

All markets can impose disciplinary actions upon a market-member for a failure to comply with rules relating to DEA. A number of different penalties can be applied, ranging from warnings (for less severe violations) to the revocation of the permission to trade. In some cases, the market can require the market-member who is an intermediary to deny DEA access to a particular Customer or to exclude a particular Customer from using the system for a certain time.

However, many markets have expressed concern that they do not have the authority and, therefore, lack of the ability to take disciplinary actions directly against non-members, e.g., the DEA Customers of members. The concern expressed was that even though market rules may provide that market-members are responsible for their Customers' trading through DEA, it may be difficult to prosecute an intermediary for the underlying violation of the market rules caused by the Customer. Instead, actions may be taken to sanction the market-member for a lack of supervision of trading. In fact, however, it may be difficult for a market authority to prove that the intermediary had inadequate policies and procedures in place. It should be noted, however, that in all SC2 and SC3 member countries, the relevant statutory regulator has jurisdiction over any person engaged in fraudulent trading practices on a market, whether a market-member or not.

Another factor that complicates enforcement of market rules in the DEA context is that most market electronic systems do not identify, in real time, the particular Customers of market-members who may have SA or AOR (i.e., the systems do not support sub-user identifiers or

passwords). Indeed, some markets permit the sub-delegation of a Customer's DEA access to another party.

In their responses to the consultation/survey, some intermediaries stressed the importance of trading risk and that the market authority will hold the intermediary responsible for the violation of any trading rules imposed by the market. One North American intermediary expressed particular concern about possible violations of SEC or other rules pertaining to trading conduct – for example, improper trading designed to manipulate the closing price. As the intermediary for such a trade, it will be held to account for any problematic trading activity performed by its Customer.

Most intermediaries enter into written contractual agreements with their DEA Customers, the purpose of which is to restrict, condition or otherwise control how those DEA Customers utilizing the intermediary's infrastructure to transmit orders, as well as to seek to ensure compliance by their DEA Customers with market rules. Some of the key terms and conditions contained in such contracts include the following:

- Provisions that address the respective rights and liabilities of the parties such as statements that the Customer accepts all liabilities resulting from DEA (including use of identification codes, settlement and delivery);

- Provisions relating to the security (physical and IT security) of the infrastructure (user identity, passwords, authentication codes, etc.), to avoid unauthorized system access;

- Limits that are expressed as a notional amount for each Customer above which the orders are rejected by the system, as well as by reference to the maximum amount per order/per user;

- Warranties, indemnities, charges and Customer/product specific conventions;

- Conditions (such as for entering orders, error trade policies, etc.) and restrictions such as the right to suspend the service, to reject or cancel orders, etc.;

- A requirement to have knowledge of trading rules and applicable laws and regulations or a requirement to comply with these; and

- A requirement that the Customer's personnel who manage the process are authorized, qualified and competent.

These terms and conditions are usually standard in terms of restrictions, conditions and controls although most intermediaries clarify that they are adapted to the business relationship with the Customer and the type of service provided (dealing services, clearing services, prime brokerage).

In addition, most intermediaries are required to have in place proper procedures and policies to monitor DEA Customers and their trading activities. However, even where intermediaries have in place appropriate procedures, in certain cases, market rule violations have occurred nonetheless.

B. Risk Management

Credit risk is a key risk management concern. It is generally described as the risk that an intermediary is normally financially responsible for the trades of a Customer. Some industry representatives at meetings sponsored by IOSCO in the research phase of this project emphasized that non-clearing market members presented essentially the same type of *credit risk* to a clearing firm as a DEA Customer of an intermediary.

As an example, one North American based firm indicated that compliance or regulatory risks are more pronounced when a DEA Customer that is not a market-member places orders directly on a market in the name of the intermediary, and that credit risks are more pronounced where the DEA Customer is not a clearing member of the market.

In most jurisdictions, primary responsibility for overall credit control and risk management, including with regard to DEA, is the responsibility of the market-member and the market member's clearing firm, and the clearance and settlement (C&S) entity,[10] but *not* the market. Although C&S entities do not assume *per se* the risk management obligations of intermediaries specifically with regard to DEA, they do play an important supporting role. The C&S entity will have systems in place to manage risk, including the imposition of trading and position limits, the setting of margin requirements, as well as collateral control and monitoring the financial health of its clearing members.[11]

Where there is automated order routing, i.e., where orders are sent through the intermediary's infrastructure, the intermediary has the opportunity and time to implement its risk management protocols, including pre-trade controls. However, even then, the speed of electronic execution narrows to milliseconds the available time for traditional risk management and error trade detection and response. In SA situations, i.e., where orders are transmitted to the exchange trade matching system outside the intermediaries' infrastructure, the ability of the responsible firm to conduct robust risk assessment, particularly on a pre-trade basis, is even more limited in the absence of risk management functionalities software engineered into the execution path to the markets. This magnifies the potential negative effects of a mistake (e.g. errant algorithm) or of a DEA Customer exceeding credit limits.

Although competition appears to be driving major markets to implement the risk management tools desired by intermediaries,[12] differences remain in the risk management functions made

---

10 The term *clearance and settlement entity* refers in general to both a central counterparty, e.g., the National Securities Clearing Corporation located in the United States, and a central securities depository, e.g., the Depository Trust Company and Clearing Corporation, also headquartered in the United States.

11 In a previous report, IOSCO noted that a central counterparty has the potential to reduce significantly risks to market participants by imposing more robust risk controls on all participants and, in many cases, by achieving multilateral netting of trades. It also tends to enhance the liquidity of the markets it serves, because it tends to reduce risks to participants and, in many cases, because it facilitates anonymous trading. See http://www.iosco.org/library/pubdocs/pdf/IOSCOPD176.pdf.

12 Eurex trading platform release 11.0 combines trading (order entry), risk management (risk exposure, including the ability to stop specific traders from continuing to trade) and post-trade clearing (margin, settlement netting) functionalities. See http://www.eurexchange.com/r11/functional_features_en.html. Among other things, Eurex permits members to trigger a "stop" action on individual trader IDs, which encompasses both individuals and algorithms that run under specific trader IDs. Triggering a *stop* action will make it impossible for the Trader ID to engage in any further trading activities and will

available by markets and C&S as part of their electronic trading systems. The regulatory issue is whether market authorities should specifically identify the type of controls (e.g., filters) that trading systems should make available for risk management purposes.

Some markets articulate high level principles setting out broad risk management expectations, and require market-members offering DEA to their Customers to implement procedures that are intended to achieve certain risk management objectives, but do not impose any detailed or specific parameters to achieve such objectives. By contrast, other markets set forth more detailed expectations. For example, they may enumerate a list of expected controls, such as monitoring capabilities and the ability to set credit control parameters (e.g., trade quantity limits, position limits, exposure limits, loss limits, and eligible products and instruments), and the ability to adjust control values and parameters in real time during a trading session.

Intermediaries appear to manage the risks posed by DEA using a three-pronged approach:

1. an analysis of the potential DEA Customer (e.g., history, creditworthiness, etc);

2. pre-execution risk controls; and

3. post-execution controls.

Each of these three mechanisms must work together to provide a comprehensive risk management program.

Of the three risk management tools available to the intermediary, the first - analysis of the Customer- is sometimes described by intermediaries as the most critical, since it is not possible to impose meaningful pre- and post-execution risk control measures unless the intermediary has a comprehensive understanding of the DEA Customer's risk profile.

All intermediaries who responded to an IOSCO survey reported monitoring trades on both a pre- and post-trade basis, but such monitoring took various forms. Moreover, some intermediaries that require their Customers to use the intermediaries' infrastructure indicated that one of the reasons for not permitting *sponsored access* was due to the inability of the intermediary under such circumstances to impose sufficient pre-execution risk controls.

Most intermediaries reported that pre-trade controls, at a minimum, included protection against orders placed in error, sometimes referred to as *fat finger* protections. Other common pre-execution controls included *abnormal activity* alerts, and filters that provide for a maximum order size. Some controls are designed to respond promptly to increasing risk presented by a DEA Customer's trading pattern. Others do so by setting trading limits on size of orders, credit or total margin exposure, or maximum order and total value of an order. The limits may restrict further order flow when breached.

A number of intermediaries stated that if a Customer reaches a trading position that is close to the total limit set for the Customer, they have the ability to reduce the frequency and/or size

---

delete all open orders preventing any increase in risk of that trader ID. See http://www.eurexchange.com/r11/functionalfeatures/risk/stop_button_en.html.

of subsequent orders, in order to prevent subsequent Customer orders from going over the pre-set limit. Such tools may be particularly relevant with respect to Customers using automated algorithms to place orders on a market. In addition, intermediaries generally have the ability to press a *stop* or *panic* button, in order to prevent a DEA Customer from placing any further orders on the market.

Additional pre-trade execution controls appear to be coming into use. For example, some intermediaries reported that they now have the ability to see pending order flow placed by their DEA Customers, but not yet executed on the market. Still other intermediaries are developing the ability to delay orders in order to run a pre-execution filter, so that after a DEA Customer places the order, the intermediary's automated systems will have a period up to one second in which to reject the trade. However, one European respondent noted that it would not be possible to impose *systematic limits* on DEA Customers on orders if those transactions did not flow through the intermediary's infrastructure.

Pre-execution trading filters are common in AOR. In such cases, the intermediary has the ability to see the order flow and interact, i.e., it can stop an order before execution. However, in SA, the use of such filters appears to be less prevalent. A common theme through the responses was that DEA Customers would not accept any filter that imposed a delay in order execution. Intermediaries face pressure from DEA Customers, especially, high frequency traders, to be able to trade without pre-trade filters which may add latency. Acceptance of this practice would provide an incentive for intermediaries to eliminate what can be a valuable risk management and market integrity protection tool in order to accede to the demands of DEA Customers seeking a latency advantage, albeit in milliseconds.

On the other hand, some C&S and intermediary representatives argue that risk management should not be viewed in terms of a *one-size-fits-all* series of mechanical actions and that responsible risk management approaches can appropriately rely more heavily on robust *know your customer* inquiries and *post-trade* controls rather than on pre-trade filters. Some intermediaries and market representatives have noted that a mechanistic rejection of an order that exceeds a *hard* trading limit without knowledge of the Customer's entire trading strategy and positions in other instruments could inadvertently convert a winning trade into a losing position.

In effect, those arguing for a flexible risk management approach believe that responsible risk management decisions cannot be reduced to a formula, but must be the result of an active, case-by-case decision-making process that takes into consideration the distinct characteristics and sophistication of the DEA Customer. Under this approach, it is argued that an intermediary might rely more heavily on credit determinations and the sophistication and background of the Customer, along with past experience with the Customer, rather than on pre-trade controls that set hard limits on order quantities, and that therefore pre-trade controls might vary. For example, a pre-trade filter may be used to trigger a warning rather than impose a cap on orders.

Nonetheless, it should be recognized that technological advances have minimized the latency effects of pre-trade filters, a key risk management tool. Accordingly, this raises the issue of whether markets should make certain pre-trade filters and post-trade functions available as a matter of best practice in order to facilitate better risk management at the firm level.

All surveyed intermediaries confirmed that they monitor trades on a post-trade basis. One European firm reported applying an in-house developed risk management model over the aggregated position in addition to applying various limits such as credit risk, stress risk, concentration risk and long option premium limits. There was however, a varied approach in terms of applying post execution controls.

C. Adequacy of Information from the Market and/or Clearinghouse

The surveys undertaken by IOSCO highlight that intermediaries that permit Customers to use SA in order to execute transactions do not always receive information concerning pending orders on a pre-execution basis. As an example, one North American intermediary stated that "to the extent that Customer transactions [are] on a sponsored access basis, the Customer's orders are not visible to it before execution, other than through supervisory terminals made available by connectivity providers/service bureaus."

By contrast, other intermediaries emphasized their ability to obtain information on a near real-time pre-trade basis, sometimes referred to as *drop-copy*.[13] In theory, the order is not yet executed, but in practice there is generally no way to stop the order once the *drop copy* has been received.

Issues relating to post-trade data appear to be less acute than with respect to pre-trade information. Intermediaries generally reported that they are able to obtain information on a post-trade basis for their DEA Customers that is identical to, or substantially the same, as for clients trading on a non-DEA basis, i.e. full trading details (type, instrument, price, quantity, time, etc.). With very few exceptions, data is received immediately following the trade (once every 5 minutes at the latest, depending on the market). Speed of data appears to depend on the mode of access and electronic line/connectivity used by DEA Customers.

D. Algorithmic Trading and Co-location

The overwhelming majority of markets responding to an IOSCO survey question on capacity issues indicated that they had no concerns about capacity; however, a smaller number expressed capacity and system response concerns related to algorithmic trading. While algorithmic trading has the potential to enhance the quality of the market through increased trading interest and resulting price discovery, it also can potentially overwhelm system capacity and force delays in order display and execution through the queuing of messages.

The Consultation Report raised the issue of whether differences in latency arising from different means of connecting to trading systems and locating trading systems close to exchange servers (i.e., so-called *co-location*) raise any concerns that should be addressed by means other than disclosure and equitable access as provided for in *IOSCO's Principles for the Oversight of Screen-Based Trading Systems.*[14] In that report, we stated that *equality of*

---

13 In general, this refers to the intermediary receiving a *copy* of its SA Customer's order as it is placed for execution.

14 *See Principles for the Oversight of Screen-Based Trading Systems*, Report of the Technical Committee of IOSCO, June 1990 (Screen-Based Principles Report); and *Principles for the Oversight of Screen-Based Trading Systems for Derivative Products-Review and Additions*, Report of the Technical Committee of IOSCO, October 2000, at p. 5, section III, Part 1, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD111.pdf.

treatment within a given connectivity option was most important and that *differences in response time should be addressed by disclosure.* Not all respondents addressed this issue and of those who did, the comments were split equally.

The comments indicating that they were content with the disclosure and equitable access approach generally viewed the issue in the context of providing Customers with access that is appropriate to each Customer's business model. Respondents whose latency concerns were not fully addressed by disclosure and equitable access generally emphasized the need for fair and equitable access to the market for all market participants and the elimination of competitive disadvantages. However, a common theme through the responses was that DEA Customers would not accept any filter that imposed a delay in order execution.[15]

The *fairness* of latency differences resulting from different technical connection options and in particular from co-locating high speed *algorithmic* trading systems adjacent to exchange servers raises significant technical and market integrity issues. At this time, in light of the limited public comments, the Technical Committee has determined not to develop any new policy on this issue. Pending further work on this issue, the Technical Committee suggests that market authorities take into account the approach set out in IOSCO's earlier paper relating to the *Principles for the Oversight of Screen-Based Trading Systems.*

The combination of DEA and algorithmic trading can, on rare occasions, pose threats to orderly trading. Markets should, as appropriate, adopt, and implement on an automated basis, measures to address such threats.

---

15 Some intermediaries indicated that the filters had not slowed order execution. Another broker acknowledged that filters could slow the order process, and indicated that it was working on enhancements to its filtering tools so that it would not add to the *latency* period in order execution. Another firm indicated that where filters are implemented "appropriately," there is only a minimal latency period.

Chapter 5 Principles for Direct Electronic Access with Explanatory Text

A. Introduction

As a preliminary point, the Technical Committee notes that whether to allow the use of DEA is itself a regulatory question and that not all jurisdictions may believe that it is appropriate to do so. The Technical Committee expresses no opinion as to whether a jurisdiction should allow the use of DEA. This Final Report is intended as guidance for jurisdictions that do allow or are considering whether to allow DEA.

As indicated in this Final Report, markets and intermediaries that are market members should have appropriate policies and procedures in place that seek to ensure that DEA Customers will not pose undue risks to the market and the relevant intermediary, and regulators should take measures to ensure that such policies and procedures are in place. The increasing use of DEA has, however created, substantial challenges. For example, there is the potential, particularly if proper controls are not implemented, that a Customer may intentionally or unintentionally cause a market disruption or engage in improper trading strategies that may involve some elements of fraud (including manipulation), and/or that may expose the intermediary to excessive credit risk. Unauthorised access is also generally recognised as being a major concern in terms of market integrity and security.

In light of these facts, the Consultation Report contained eight principles applicable to DEA arrangements in three key areas:

(i) pre-conditions for DEA;
(ii) information flow; and
(iii) adequate systems and controls.

Some of the proposed principles were modified in response to comments raised by stakeholders and concerns raised by regulators. A feedback statement that summarizes the comments received and the responses of the Technical Committee is attached to this Report as Appendix 2.

This section of the Final Report sets forth the final principles and describes the central risks that each principle seeks to address.

B. 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 with, 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.

This principle addresses the risks posed by allowing any user to access markets outside of the infrastructure and/or control of market intermediaries' traditional risk management approaches. In particular, allowing such access may make rule compliance and monitoring more difficult (e.g., regarding market manipulation and insider dealing.)

This principle is not intended to indicate whether a market authority should prescribe rules establishing minimum customer standards in the DEA area or, conversely, whether the primary responsibility for compliance should be with the intermediary and the markets, leaving the regulator in a supervisory role. The Technical Committee recognizes that each jurisdiction will determine its own mechanisms for determining minimum standards for Customers.

The principle does not imply that the intermediary must review each DEA customer's particular knowledge of the market rules and proficiency in the order entry system. However, the Technical Committee believes that firms should, as a matter of sound risk-management, take reasonable steps, such as requiring certain representations or warranties, as appropriate, during the customer vetting process, to confirm that the DEA customer is taking reasonable and appropriate steps to ensure that it has both sufficient knowledge of the market rules and technical proficiency in the trading system. Once again, the Technical Committee recognizes that it is the decision of each jurisdiction as to whether such steps should be left entirely to firms' individual determinations or whether regulators should take a more active role is establishing minimum steps for customer vetting.

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 between itself and the DEA customer.

The Technical Committee's inquiry into DEA revealed substantial variation in the procedures used by markets and intermediaries to authorize DEA and ensure the ability to sanction improper conduct. A fundamental concern raised by customers' use of DEA is the need to ensure that the intermediary's customer will comply with market rules. Although the intermediary remains ultimately liable for all market rule compliance (see below), as a practical matter, such compliance will be facilitated through legally binding requirements on a DEA customer.

In addition, concern had been expressed that, even though market rules may provide that market members are responsible for their customers trading through DEA, it may be difficult in some jurisdictions to prosecute an intermediary for the violation of the market rules caused by the customer. A contractual relationship between the market and DEA Customer is one of several ways to enable market authorities to enforce rules directly against the DEA Customer.

However, the Technical Committee believes that it should be left to individual jurisdictions to determine whether their regulators should establish requirements governing the legal relationships between markets, intermediaries, and DEA customers.

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.

In those jurisdictions where a DEA customer is permitted to sub-delegate its direct access privileges to another party (a sub-delegatee), the intermediary continues to be ultimately responsible for all orders entered under its authority by the sub-delegatee 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.

Principle 3 addresses the issue of ultimate responsibility for DEA arrangements, including where access rights by a DEA customer are *sub-delegated* to a third party. Of particular concern, in the absence of contractual or other measures, is that sub-delegation makes it difficult for the responsible intermediary to identify a sub-delegatee.

The principle emphasizes that an intermediary retains *ultimate responsibility* for all orders under its authority. The revised principle removes any implication that IOSCO is endorsing the practice of sub-delegation. However, should the intermediary choose to assume the risks associated with sub-delegation, and presuming that the practice is permitted by the intermediary's supervisory authority, the intermediary remains ultimately responsible for all orders entered into by the end user of a DEA customer's system and should employ some means to assure that the DEA customer knows all its sub-delegatees.

C. 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.

A factor that complicates enforcement of market rules in the DEA context is that most markets' electronic systems do not identify the particular customers of market-members who may have SA or AOR (i.e., the systems do not support sub-user identifiers or passwords). This may delay the process of investigation if the market authority seeks information to identify the ultimate customer or user. Additional complicating factors include increased volume and the complexity of information caused by algorithmic trading.

The Technical Committee believes that the intermediary must know who is using its DEA facilities and have in place procedures for identifying any sub-delegates, if sub-delegation is permitted. The principle requires that means be employed by the intermediary to identify the client having sent any DEA order, at the market authority's request, to facilitate market

surveillance.[16] The Technical Committee believes that assigning each DEA customer a unique ID or mnemonic is not a novel concept. The use of unique IDs is related to two goals: identifying the person or system that entered an order and identifying the beneficial owner of that order. An ID unique to each DEA customer or sub-delegatee authorized to enter orders will identify that person or system and facilitate efforts to determine the beneficial owner of the order.

Principle 5: Pre- and Post-Trade Information

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.

This principle reflects the Technical Committee's recognition that in the dispersed world of electronic trading, intermediaries must have timely access to relevant pre- and post-trade information in order to facilitate the performance of their traditional risk management functions in the context of DEA.[17]

D. 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.

Whatever the maximum level of risk that a firm accepts may be, it must not be infinite. Neither the perceived sophistication of the firm, its risk management expertise nor its access to funding warrants exposing its clients and a clearing organization to unlimited risk. Accordingly, the Technical Committee concludes that firms must have the electronic controls to limit their risk exposure in order to protect customers and the clearing organization.

The Technical Committee believes that the specific type of pre-trade controls implemented by a firm or market that enable intermediaries to implement appropriate risk limits should be

---

[16] The Technical Committee recognizes the importance of maintaining the confidentiality of certain information as well as the need to use such information consistent with a supervisory or regulatory purpose. Market authorities should implement the principle based on regulatory requirements and business practices applicable to their respective jurisdiction. *See also* the attached Feedback statement under Industry Feedback (Appendix 2 pages 8-9).

[17] Id.

a matter for determination by the market, market intermediaries, clearing firms, and market authorities. Intermediaries already make such determinations; and the Technical Committee is not taking a position as to the level of granularity with which market authorities should regulate those determinations. Nonetheless, with regard to the implementation of such pre-trade controls, it is the intermediary's (including a clearing firm's) responsibility to help ensure that the controls it is using are effective when implemented and on an ongoing basis.

The use of electronic controls to limit the level of risk that an intermediary accepts is particularly necessary in the context of high speed algorithmic trading. A firm default exposes all of its customers to loss, as well as the clearing organizations of which the firm is a member, and could have broader systemic effects. The suggestion that a customer's true position may include offsets of which the firm is unaware is insufficient to permit the customer to place unlimited positions.[18] The Technical Committee recognizes that these possible effects of a firm default raise significant regulatory issues.[19]

DEA also raises issues concerning the financial condition of the clearing firm. The Technical Committee believes that a clearing member has the same need to be able to control its exposure to the trades it clears for a market member as it does with respect to its own AOR or SA customers or those AOR or SA customers of another intermediary. The Principle clarifies, by including "as appropriate" in the parenthetical text relating to clearing firms, that where a separate entity is undertaking the clearing arrangement for a DEA intermediary, the clearing firm should require that automated pre-trade controls are in place to control the risks posed by the market intermediary. While the clearing firm is not directly responsible for managing the risk posed by individual DEA customers of the market intermediary, the clearing intermediary should manage the risks posed by the market intermediary's DEA customers as a group, as well as those risks posed by all direct DEA customers of the clearing firm, as the clearing intermediary is responsible for all trades it clears.

As discussed above, the Technical Committee believes that the specific type of pre-trade controls implemented by a firm or market that enable intermediaries to implement appropriate DEA risk limits, including the particular technology or structure by which such controls are achieved, should be a matter for determination by the market, market intermediaries, clearing firms, and market authorities.

As one example, a market could, with regulatory approval as necessary, provide and operate an automated system (i.e., software and hardware) that is used (i.e., by the setting of risk limits) by each of (a) the market intermediary, to limit the risks posed by its DEA customers individually and (b) the clearing firm, to limit the risks it clears, including those posed by

---

18 The fact that the intermediary may be unaware of risk-reducing positions held by the customer implies that the intermediary may also be unaware of risk-enhancing positions. Moreover, in the event of the insolvency of the customer, gains from risk-reducing positions may not promptly be available to meet losses on positions held through the intermediary.

19 For example, some regulators take the position that an intermediary may not obscure risk management, meaning that the intermediary would not be able to rely on a third party to establish and administer risk parameters on behalf of the firm. This paper does not support the outsourcing of the intermediary's risk management responsibilities. In fact, by focusing on providing appropriate tools to the intermediary, some of which may be provided by the market, the above principles are intended to promote the implementation of appropriate risk management procedures in the DEA context.

market member DEA customers, by non-market-member DEA customers and by a market intermediary's DEA customers on an omnibus basis.

As a result of comments received on the Consultation Report, Principle 6 was modified to clarify that it applies to all three DEA pathways in order to complement principle 7, which essentially states that intermediaries, including clearing firms, should use both regulatory and financial controls to be used in connection with DEA trading. Controls to credit risk should limit or prevent a customer from placing an order that exceeds (or causes a non-clearing intermediary to exceed) existing position or credit limits. There is no convincing rationale for not using automated credit limit system filters, particularly when the failure to use such automated filters may expose market participants to unacceptable risks. In order to implement controls, it will be critical for intermediaries, third party vendors and markets to cooperate in putting into place appropriate systems and controls.

Principle 8: Adequacy of Systems

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

Because of the impact systems failures have on public investors, intermediary exposure, and market efficiency, the Technical Committee believes that it is necessary for market authorities to take appropriate steps to obtain assurance that the automated systems of intermediaries and markets operate properly, and have the adequate capacity, scalable to volume,[20] to accommodate trading volume levels and to respond to emergency conditions that might threaten their proper operation. In particular, market authorities should require intermediaries and markets to establish comprehensive planning and assessment programs to test systems capacity and security and to ensure that they possess the appropriate technical expertise to maintain and operate these systems. The programs should include:

1) the establishment of capacity estimates for their automated order routing and execution, market information, and trade comparison systems;

2) periodically conducting capacity stress tests to determine the behavior of automated systems under a variety of simulated conditions;

3) seeking on a periodic basis the assessment of independent reviewers with regard to whether these systems are performing adequately and whether these systems have adequate security; and

4) implementation of policies for the hiring and training of qualified technical personnel.

[20] The term *scalable* refers to the ability of an intermediary or a market to increase efficiently capacity as volume increases.