FUTURES AND OPTIONS ASSOCIATION

GUIDANCE ON SYSTEMS AND CONTROLS FOR ELECTRONIC TRADING ENVIRONMENTS

SEPTEMBER 2012

Version 1

Index **Page No.**

1. Introduction by the FOA

1.1. The purpose of financial markets is to serve as a means of raising capital, facilitating savings and investment and enabling corporates and investment firms to manage their various business risks. Since financial and commodity markets first emerged, three key ingredients have enabled market participants to achieve these objectives with maximum efficiency - fast access to information and market data, proximity to the market, and speed of execution. As the rate of technological development increased and markets converted from open outcry to electronic, so market participants became increasingly more dependent on electronic systems with fast and versatile trading engines to optimise their services.

1.2. This new technology has reduced transaction times, created more efficient electronic audit trails, improved risk controls and enhanced market monitoring. It has also seen the emergence of algorithmic trading (where orders are generated according to pre-set programmes) and a low latency variant of algorithmic trading known as "High-Frequency Trading" (**HFT**).

1.3. HFT has grown rapidly in recent years but because of its broad scope and wide number of differentiated strategies, it is difficult to define in any meaningful way. HFT does have a number of common features however, such as the use of sophisticated technology, extensive use of algorithms and a high turnover. In addition, positions are typically held for short periods of time.

1.4. The FOA recognises the widespread concerns associated with these activities, and supports the desire of regulators around the world to find ways to minimise risks posed by them. It is against this background that the Futures and Options Association (**FOA**), with considerable input from its E-trading / Risk Working Group and Sam Tyfield, Partner of Katten Muchin Rosenman UK LLP, has developed this Guidance.

1.5. This document supports and seeks to provide more detailed guidance on the implementation of, amongst other things, the '*Guidelines on systems and controls in an automated trading environment*'[1] (**ESMA Guidelines**). In recognition that European derivative markets are largely electronic, the Guidance addresses systems and controls as they relate to electronic trading. The FOA considers this broad approach necessary to ensure that controls across markets are sufficiently robust.

1.6. The purpose of this document is to:

(a) Establish a standard for members to judge the appropriateness of their own control environments in relation to the ESMA Guidelines;

(b) Clarify the obligations and responsibilities that market participants have to one another, to their respective regulators and to the market as a whole;

(c) Establish example documentation and information required to be provided between industry participants to assist in the efficient but safe operation of the markets; and

1 ESMA 2012/122, 14th February 2012, http://www.esma.europa.eu/system/files/esma_2012_122_en.pdf

(d) Explain how the industry is implementing the ESMA Guidelines in practice to ensure there is an appropriate control environment to minimise the risks posed by electronic trading.

1.7. The FOA will review this Guidance periodically to take account of future market or regulatory developments.

Blake Stephenson
Regulation Manager
Futures and Options Association

2. Introduction by the FOA E-Trading / Risk Working Group Chair

2.1 On behalf of the FOA E-Trading / Risk Working Group I am pleased to present this Guidance on Systems and Controls for Electronic Trading Environments.

2.2 The FOA E-Trading / Risk Working Group has been working diligently with industry members and stakeholders to deal with concerns which have been raised recently regarding systemic and other risks posed by high frequency and automated trading on global markets, with particular emphasis on the EU.

2.3 There are a number of legitimate concerns arising from continued technological developments in electronic trading. To mitigate these risks whilst maintaining market efficiency, the industry continues to focus investment on market surveillance, risk management and monitoring systems. It is therefore preferable that these systems and the obligations and duties related to them, are discussed and developed by the industry itself, bearing in mind the regulatory context, such as the ESMA Guidelines on automated trading and the review of MiFID being undertaken.

2.4 This industry is fluid, dynamic and innovative. Our intention has been to deal with the concerns within the industry, among regulators and politicians, and the general public in a way which protects market integrity without stifling a successful and beneficial industry. We will continue to work with industry participants and other stakeholders to develop this Guidance as markets and technology evolve.

Paul Marks
Chairman
FOA E-Trading/Risk Working Group

3. Use of this Guidance

3.1 This Guidance uses terms such as “obligations” and “requirements” throughout. These terms do not impose any legal or other obligations or requirements upon market participants (as defined in this Guidance). This Guidance is intended to provide market participants with a helpful basis for the development of policies, controls and procedures.

3.2 The guidance, tools and information contained in this document provide a useful implementation standard but should be adapted so as to be proportionate to a firm’s size and strategy. Firms should read this Guidance alongside, and take their initial lead from the ESMA Guidelines directly and, in the event of any doubt, should seek independent legal or specialist technical advice as appropriate. This Guidance should not be read prescriptively; firms could demonstrate that they are complying with the spirit of the Guidance using alternative methods, policies or procedures.

3.3 At various points throughout this Guidance, reference is made to example policies and procedures which are appended at the back of this document. The adoption of the policies and procedures in the form or detail suggested will not be appropriate in every case; the appropriate form and content of each firm’s policies and procedures will depend on their individual circumstances and their trading strategies and styles. The intention is to provide FOA members with an example structure to help develop their internal policies and procedures. For ease of inclusion in this Guidance, the policies and procedures appear in table format; policies and procedures may, in practice, be automated or take such form as the relevant market participant finds most practical for use and recording.

3.4 Definitions used in this Guidance.

Except where expressly set out in this Guidance, the following capitalised words and phrases shall have the definitions set out below:

- **DEA** means direct electronic access services (including (a) use of Venue ID or Venue membership, (b) direct market and sponsored access and (c) automated order processing);

- **DEA Providers** means Members that provide clearing services and/or DEA for Members and non-member clients (collectively, **Clients**);

- **Members** means NCMs, DEA Providers, GCMs and FCMs and firms which are subject to the rules of a Venue by using a Member’s Venue ID;

- **Service Providers** means third party firms including Independent Software Vendors (**ISVs**) that provide services, including trading systems, data feeds, risk management systems and processing systems to other participants; and

- **Venues** mean, collectively, exchanges and MTFs.

4. General background

4.1 Market Structure

4.1.1 The markets to which this Guidance make reference consist of four main groups of participants:

(a) Venues;

(b) DEA Providers;

(c) Clients; and

(d) Service Providers.

4.1.2 Some of these participants will themselves be authorised by local or overseas regulators. Others, for example Service Providers, will not be regulated as they are not likely to be conducting regulated business.

4.1.3 Those participants which are authorised will have obligations and duties imposed on them by their relevant competent authority. This Guidance does not duplicate, extend or otherwise supersede those obligations.

4.2 Proportionality

4.2.1 Some or all of the requirements may not be appropriate to satisfy in every case. For example, it may not be relevant or realistic for a DEA Client with low volume or infrequent trading to meet all the requirements set out below.

4.3 Market Abuse and Manipulative Practices

4.3.1 It is in the best interests of all market participants that abusive and manipulative practices are identified as soon as possible and notified to the relevant authorities. All market participants understand that they have an obligation to report these practices to their relevant competent authority and market participants therefore are sensitive to the importance of using the tools and information available to them to identify and prevent market abuse and manipulation.

4.3.2 It is increasingly difficult, given the fragmentation of the market and the use by market participants of a number of counterparties in their trading activities, for any one market participant or group of market participants to take the sole responsibility for identifying market abuse or manipulative practices. All market participants will use their best endeavours, including where appropriate, automated surveillance/alerting functionality, to monitor for and identify market abuse and manipulative practices on an on-going basis. Appropriate surveillance products are available to purchase from third party suppliers and/or may be developed in-house.

DETAILED GUIDANCE

5. Venues' requirements of Members

5.1 Venues requirements will be Venue-specific and the rules will be contained in the relevant Venue's rulebook and membership pack.

5.2 Venues should be able to request sufficient information from DEA Providers to satisfy themselves that the DEA Providers' Clients operate according to the standards in the Guidance.

5.3 General Administration Requirements

5.3.1 Upon application for membership, Venues will place a degree of reliance on an applicant's status as an authorised person but in addition, may perform due-diligence on its soundness and fitness for membership. Soundness and fitness for membership should focus primarily on internal systems and controls.

5.3.2 Applicants which are not authorised and regulated by an EU competent authority will be required to provide more information than those which are authorised and regulated in the EU. Venues may require information to give them an overview of the firm's business for the purposes outlined above, but the Venue will not ordinarily be concerned with internal affairs such as remuneration of individual staff or profit and loss projections.

5.3.3 In the event that the Venue has concerns about the business plan or model (in particular, in applications from firms which are not regulated or authorised by an EU competent authority), the Venue will discuss this with the applicant and may insist on amendments to the business plan, with evidence as necessary, before approving the application for membership. Such amendments should focus on the applicant's ability to satisfy its anticipated financial, trading and risk management obligations on an on-going basis.

5.3.4 Venues will not seek to arbitrarily change their approach to individual members (or applicant firms) and will follow their own publicly available policies and processes in determining the form and substance of what shall be required of any firm as regards their general administrative requirements. The Venues' approach to each applicant or existing member will however be proportionate to that member's particular circumstances.

5.4 Business Plan

5.4.1 Members should have a business plan, the form and substance of which will vary depending on that Member's regulatory permissions. However, the industry reasonably expects a three to five year plan and a summary of: (a) the separation of powers and duties and responsibilities of management; and (b) training (on Venue specific rules, market abuse and manipulation) to be included. There is a reasonable expectation that the business plan should also contain a summary of the risk function, particularly

regarding (a) separation from the trading function; and (b) segregation of the member's trading and risk systems.

5.5 Hiring and Training

5.5.1 Members should take steps to ensure that their procedures ensure that adequate due diligence is undertaken when hiring new employees. That due diligence may vary depending on each prospective employees' key tasks, but particular attention should be paid to the individuals previous activities in the industry and where possible, any regulatory investigations relating to the conduct of those individuals.

5.5.2 Members should ensure that before any users are authorised to access electronic trading systems they have had appropriate training on the system functionality and the applicable market rules and regulations.

5.6 Compliance and monitoring

5.6.1 Members should have independent output from and oversight of their risk monitoring systems, segregated from the systems used and accessed by the "trading side". The exact nature of these systems will depend on the type of firm and style of its trading.

5.6.2 Monitoring and surveillance of electronic trading systems should be on a real-time or near to real-time basis so that Members can identify unusual trading patterns which could indicate the incidence of market abuse, or other such activity that might cause a disorderly market, as soon as practically possible.

5.6.3 Where a Member uses external compliance or monitoring consultants, the Member should engage with and provide information to such external consultants as it would if those consultants were its own employees.

5.7 Trading and live-market access restrictions

5.7.1 Certain testing must be undertaken before strategies and / or algorithms are put into the live market, including for example, those tests set out in Sections 5.8 and 5.9.

5.7.2 A Member's trading systems should also be able to monitor heartbeats with the Venue to identify when connectivity to the Venue is lost.

5.7.3 A cancel-on-disconnect / don't cancel orders on disconnect policy should be developed for each Venue and each trading system, leveraging the automated Venue settings where available.

5.7.4 Both Venues and Members are responsible for providing kill button functionality. A Venue kill button or function (i.e. the ability to pull all orders *en masse*) should operate on a per login / session or per Venue ID basis to quickly suspend electronic trading if required. When a DEA Provider kill button / function is activated, all resting orders on the applicable entity are cancelled and further access suspended. An application programming interface (**API**) for the kill-button / function should be developed based on an industry standard protocol and it should be possible to access such functionality

in an automated fashion although there should be an additional manual process to pull live orders off the market.

5.7.5 A policy in relation to the use and application of kill buttons / functions must be established and where necessary, agreed with the Venues and any DEA Provider.

5.7.6 Members should have automated 'restricted list' functionality where applicable to prevent trading on products that would breach its compliance policy. Adjustments to this list should be feasible on an intraday basis.

5.8 Conformance testing

5.8.1 Members must undertake technical and functional conformance testing with the Venues which should address both trading functionality and processing market data.

5.8.2 Technical tests typically include connectivity (including cancel / don't cancel on disconnect, market data feed loss or hitting exchange throttles), recovery (including cold intra-day starts) and the handling of suspended instruments or stale market data.

5.8.3 Functional tests typically include static and market data download and all applicable business data flows between the Member and the Venue such as trading, quoting, trade reporting and other pre- and post-trade flows (e.g. risk management information).

5.8.4 Subject to Section 7.3, the process, content and timing for conformance tests (and re-testing) can be mandated by the Venue. Alternatively, Members may be given the opportunity to perform their own conformance tests which satisfy the intent of this requirement. Minor software releases, optional functionality and stress tests should not be part of the mandatory conformance tests, but appropriate and proportional testing should be carried out taking into account the themes outlined above.

5.9 Technical stress-testing

5.9.1 Members should ensure by way of periodic testing, that the systems, procedures and controls in place are capable of withstanding significant and extraordinary market pressures or external events, including but not limited to, high volumes of data or order traffic, Venue systems throttling or short-term BCP / DRP events (Sections 5.17 and 5.18). Depending on different trading models the following tests should be considered:

(a) Initiating, running and stopping a large number of models in parallel; and

(b) Repeating high volume tests while simulating unusual market events such as a market data outage, or market gateway failure.

5.10 Non-live testing environment

5.10.1 The ability to run conformance testing, stress testing, and tests to confirm how a strategy will perform in the market when live, is dependent on the availability of an adequate test environment. To require a 'near-live' testing session to be provided by a Venue will be subject to a large cost and implementation timetable, and may not always

be practicable. Technology is available for firms to simulate a live market and against which strategies can be tested. We recognise participants' obligations under law and regulation to keep an orderly market, and Members will take steps to ensure that their own strategies or trading systems will not go live in the market without first being tested and signed-off by the appropriate personnel.

5.11 Pre-trade risk controls

5.11.1 Members should be subject to pre-trade risk limits and controls[1]. Applicable Venue limits will depend on the asset class and should be available to Members both via a graphical user interface (**GUI**) and an API. Limit checking should be automated where appropriate. Pre-trade risk limits should work hand-in-hand with real-time post-trade risk checks and it should be possible for responsible persons to adjust pre-trade limits intraday. The following are examples of pre-trade risk limits that should be in place[2]:

(a) **Price collars** - prevents orders with overly aggressive limit price entering order books. Venue and DEA Provider should be able to enter a setting per product;

(b) **Maximum order value (fat-finger notional limits)** – prevents orders with uncommonly large order values from entering order books. Limits should be set in notional value with the ability to be set per product.

(c) **Maximum order volume** - prevents orders with an uncommonly large order size from entering order books. Limits should be set in shares or lots. Options exposure may be based on delta equivalent where appropriate post-trade checks are in place;

(d) **Maximum long/short positions** - prevents trading beyond a specified position threshold. Limits should be set in units appropriate to the asset class and configured per product and on a per client, group, trader or account basis;

(e) **Maximum long/short overall strategy position** (i.e. potential multi-legged orders liabilities taken as a whole) - prevents trading beyond a specified position threshold. Limits should be set in units appropriate to the asset class and configured per product and on a per client, group, trader or account basis; and

(f) **Maximum messages limit** (throttle limits) - prevent sending an excessive number of messages to order books.

NB. As an alternative to (c) above, rather than lot based limits, an aggregate intra-day or total pre-trade margin limits (where appropriate post-trade checks are in place) may be applied.

5.11.2 DEA Providers should have systems which enable Clients to comply with any pre-trade risk controls imposed by a Venue.

1 For reference, Venues' obligations are highlighted in Section 7.

2 In line with FOA's core focus, the limits and controls Section in 5.11.1 refer specifically to derivatives markets. Cash markets may be subject to other appropriate limits and controls which are not the subject of this Guidance.

5.11.3 If a Client acquires a risk management system (in whole or in part) from a third party, it is the DEA Providers' responsibility to ensure that the policies and procedures are followed as regards that third party risk management system.

NB. Under this Guidance it is a requirement of Venues to prohibit "naked" access (see Section 7.6 below). A Venue may however decide to impose, design, implement and monitor pre-trade risk checks and limits itself and provide for all Members to go through the Venue's own pre-trade risk layer notwithstanding that the Member has gone through (or may go through) another market participant's pre-trade risk limits / checks.

5.12 Post-trade risk checks

5.12.1 Post-trade checks should be applied in near real-time and should be used in conjunction with pre-trade limits (See also Section 5.11).

5.12.2 Members should consider their own proportionate levels of post-trade risk appetite. For example, a Member could set daily loss-limits by instrument, asset class, and strategy and automatically close out or reduce positions if those limits are breached. Alternatively they could monitor intra-day the margin values of client portfolios.

5.12.3 Each Client should be subject to periodic margin-checking requirements and routine stress testing by DEA Providers.

5.12.4 Post-trade risk checks should be applied to overnight portfolio exposures (including concentration risk and historical scenario stress testing).

5.12.5 Members' systems should have 'trade-with-self' prevention logic or 'trade-with-self' alerts which includes parent and / or child firm options, to assist with the identification of self or wash-trades.

5.13 Reasonableness check

5.13.1 Members should have real-time automated systems to monitor and evaluate the quality, quantity and reliability of incoming data (including the acknowledgement of orders or trades), to mitigate the risk of erroneous or repeated orders, trades or trade reporting.

5.14 Risk limits override systems / procedures

5.14.1 DEA Providers must have procedures in place for a segregated risk function to decide how to proceed and potentially over-ride or limit changes to a system limit when a Member is in breach of a limit. A record should be made of any over-rides or limit changes including the person who made and authorised the change.

5.15 Record-Keeping Requirements

5.15.1 Venues will impose record-keeping requirements on Members which are satisfactory to the Venues' competent local authority. The purpose of these record-keeping

requirements is for the Members and the Venues to ensure that the risks of market manipulation, market abuse and disorderly and unfair markets are minimised.

5.15.2 In particular, Members should retain change control policies, procedures and records. A Venue may make a request for access to those records in the event of an audit of the relevant Member by the Venue, but a Venue will not arbitrarily seek access (and will not be responsible for seeking access) at other times.

5.16 Testing of Venue to Members communication channels

5.16.1 There is an obligation of all parties in the "chain" to test the communication channels between them periodically. Telephone numbers and email addresses (primary, back-up and escalation) and communication channels should be identified and tested with the aim of ensuring that in an emergency, the correct people with the correct level of authority may reach each other in a timely fashion in order to ensure a fair and orderly market. An out of hours procedure should be put in place where applicable.

5.17 Disaster Recovery Procedure (**DRP**)

5.17.1 Each Member should have a DRP which is proportionate to the type, nature and scale of business for each firm and which is tested on a periodic basis. The overall intent is that no firm should be at significant risk of (a) losing the ability to keep and review an accurate record of its up-to-date outstanding orders, trades or positions; and (b) being unable to close-out open positions as efficiently as possible. The types and scope of risks which should be considered are set out in the example DRPs which are appended to this Guidance.

NB. Example DRP is appended to this Guidance

THIS EXAMPLE POLICY SETS OUT SOME CONSIDERATIONS AND SPECIFICS ON WHICH FIRMS SHOULD FOCUS, DEPENDING ON THEIR OWN CIRCUMSTANCES. IT IS NOT EXHAUSTIVE OR PRESCRIPTIVE IN ITS CONTENT, ISSUES OR APPROACH AND SOME OR ALL OF THE ISSUES IN THE EXAMPLE WILL NOT BE APPROPRIATE FOR ALL FIRMS. FIRMS SHOULD ADAPT THIS AS PART OF THEIR OVERALL RISK MANAGEMENT POLICIES AND PROCEDURES.

5.18 Business Continuity Plan (**BCP**)

5.18.1 Each Member should be able to demonstrate that its systems and controls are resilient to the loss of critical infrastructure or one or more key individuals at short notice.

NB. Example BCP is appended to this Guidance

THIS EXAMPLE POLICY SETS OUT SOME CONSIDERATIONS AND SPECIFICS ON WHICH FIRMS SHOULD FOCUS, DEPENDING ON THEIR OWN CIRCUMSTANCES. IT IS NOT EXHAUSTIVE OR PRESCRIPTIVE IN ITS CONTENT, ISSUES OR APPROACH AND SOME OR ALL OF THE ISSUES IN THE EXAMPLE WILL NOT BE APPROPRIATE FOR ALL FIRMS. FIRMS

SHOULD ADAPT THIS AS PART OF THEIR OVERALL RISK MANAGEMENT POLICIES AND PROCEDURES.

5.19 Business continuity management generally

5.19.1 Adopting a BCP and DRP should not comprise the entirety of the business continuity management of a firm and its business. They form only part of that management process, planning, policies and procedures for business continuity. They should be adopted and used in conjunction with other requirements in this Guidance and (in relation to firms which are regulated and authorised by a competent authority in the EU) obligations to regulatory authorities.

5.20 Strategy adoption/implementation

5.20.1 Each Member should have clear policies and procedures to ensure, so far as possible, that during the adoption of a trading strategy or algorithmic trading strategies (**ATS**), its obligations regarding the maintenance of a fair and orderly market are satisfied. The appropriate personnel should take responsibility for the adoption and implementation of such procedures, and for the sign-off that the procedures have been followed. No person should be permitted to sign-off any process if he is conflicted from doing so (for example, by having primary responsibility for the process subject to sign-off).

5.20.2 If a Member acquires an ATS or algorithm (in whole or in part) from a third party, it is that Member's responsibility to ensure that the policies and procedures have been followed and complied with either by the vendor or by the Member itself, and to provide confirmation of such upon request.

NB. Example policies and procedures are appended to this Guidance.

5.21 Trade markers / IDs allocation

5.21.1 Trade markers / ID allocation should be available to and used by, the market for trading transparency and to ensure stability. They should be used for effective risk management in the context of a firm's overall strategy.

5.21.2 ID allocation should permit market participants to be able to monitor and identify the trading activity of individuals or firms and each Member should be able to track, monitor, control and otherwise take action in relationship to each trading strategy or ATS which it has "live" in the market.

6. DEA Provider requirements of Clients

6.1 A DEA Provider may require from each Client similar information, and expect similar systems and controls to be in place, as the Client would have to provide to the Venue if the Client was a Member. The particular information, systems and controls to be expected by a DEA Provider should be proportionate to and depend on, among other issues: (a) the level of expected trading and order volume; (b) the size and complexity of the Client itself; and (c) the nature of connectivity to the relevant Venues.

6.2 If a Client acquires an ATS, algorithm or a risk management system (in whole or in part) from a third party, it is that Client's responsibility to ensure that the policies and procedures are followed and complied with either by the vendor or the Client itself, and to provide confirmation of such upon request.

6.3 Hiring and Training

6.3.1 Clients must take steps to ensure that their procedures include that adequate due diligence is undertaken when hiring new employees. That due diligence may vary depending on each prospective employees' key tasks, but particular attention should be paid to the individual's previous activities in the industry and where possible, any regulatory investigations relating to those individual's conduct.

6.3.2 The DEA Provider should satisfy itself that a Client's compliance officer / responsible person has set up internal controls to ensure that users have received appropriate training on system functionality and the applicable market rules and regulations before they are authorised to access electronic trading systems.

6.4 Registration of Client algorithms

6.4.1 Where using their own proprietary platforms, a summary of strategy approval, implementation, monitoring and suspension processes should be provided by a Client to its DEA Provider.

6.4.2 DEA Providers shall require their Clients to register their algorithms internally for strategy and orders / trades identification purposes and so that, to the extent possible, each ATS or strategy may be given its own identifier.

6.4.3 Clients should have robust internal processes for registering their own algorithms and strategies internally to ensure that the change / control policies and procedures may be followed and to identify any individual algorithms and strategies for the purposes of reporting, or other policies and procedures. The DEA Provider should be able to require confirmation that this process has been undertaken.

NB. Example policies and procedures are appended to this Guidance

6.5 Technical Stress-testing

6.5.1 Where using their own proprietary platforms, Clients should use a non-live testing environment to check their messaging and trading systems in circumstances where

there may be throttling of orders or exceptional message flow to the Venue. This testing environment is intended to ensure that activities by participants are unlikely to harm market stability or other participants. This testing is not intended to cover exceptional error testing, which would form part of conformance testing (Section 5.8). Where using a third party (i.e. non broker provided platform) to conduct this testing, it is the Client's responsibility to ensure that adequate testing has taken place.

6.5.2 Each Client should be subject to periodic margin-checking requirements and routine stress testing.

6.6 Testing of DEA Providers to Client communication channels

6.6.1 The Client and the relevant DEA Provider share the responsibility to test communications. Telephone numbers and email addresses (primary, back-up and escalation) and communication channels should be identified and tested with the aim of ensuring that in an emergency, the correct people with the correct level of authority may reach each other in a timely fashion in order to ensure a fair and orderly market. An out of hours procedure should be put in place where applicable.

6.7 Limits / Cut-offs (including any automation)

6.7.1 Confirmation is required between the DEA Provider and its Clients that there is a process in risk control management for limits / cut-offs to be implemented and observed, (and which are agreed during the on-boarding and pre-trading process). Firms should automate risk management tools where proportionate and appropriate to do so.

6.8 Suspension of access procedures and testing

6.8.1 The requirement is for confirmation that, between the DEA Provider on the one hand and its Clients on the other, there is a process in risk control and management for suspension of access procedures to be implemented and observed. The procedures themselves may be tested prior to live trading.

6.9 Post-trade risk checks

6.9.1 Post-trade risk checks should take into account, where applicable:

(a) All electronic and voice executed order flows;

(b) Position, cash and collateral monitoring (start of day, intraday, end of day);

(c) Working as well as filled orders;

(d) Give-ins and give-outs; and

(e) Allocation instructions.

7. Members' requirements of Venues

7.1 The Venues shall ensure that their rules, systems and procedures provide for at least the information and restrictions set out in this Section.

7.2 Market / tick data access for testing

7.2.1 Access to data should be open, fair and available to all. To the fullest extent practicable the type, number or location of portals / pipes to which firms have access is irrelevant as regards quality and timing of release of data streams per portal / pipe at source.

7.3 Conformance testing

7.3.1 As far as possible, Venues will make data sets and other access available for Members to replicate a 'live' trading environment against which they can test their ATS and any modifications or changes.

7.3.2 Venues should provide a conformance testing system which should have a number of characteristics:

(a) Easily accessible, ideally on the same system as the Venue test service, and with a consistent list of instruments in the conformance testing system that are look-a-like to instruments in the live environment;

(b) Offer a self-certification front-end allowing unusual scenarios to be simulated;

(c) Available during general market hours or on a regular periodic basis even if outside market hours, ideally with the option of a dedicated or scheduled testing time per Member (to avoid conflicts between testing sessions);

(d) Supported by competent technical support staff; and

(e) Produce a summary and communicate the outcome of the conformance test to the Member (or its Service Provider). The summary should include the software version tested and a list of the functions conformed. This should be retained by the member (or Service Provider) conducting the test.

7.4 Systems resilience

7.4.1 It is accepted that a Venue may not wish to disclose its systems capacity. However, a Venue will make it known to the market through published alerts or reports where a systems resilience related event has occurred which is likely to, or has had, an impact on a fair and orderly market.

7.5 Venue kill button / function

7.5.1 There should be a kill function for all Members. This functionality should be capable of operating on a per login / session basis or per Venue ID. When activated, resting orders should be cancelled and new orders prevented from entering the market

until there is a manual reset. The function should be accessible via both a Venue provided GUI and / or an industry standard API.

7.5.2 Venues will maintain the right and ability to prevent or stop a firm trading on it under certain conditions. These conditions include but are not limited to, risks to market stability, unusual trading patterns, or loss of contact with personnel at the relevant firm.

7.5.3 Pre-trade position limits should be accessible via a Venue provided GUI and / or standard API interface.

7.6 ”Naked” access is prohibited explicitly.

7.6.1 Venues shall not permit “naked” access.

7.6.2 In the FOA’s view, “naked” access means that the relevant firm does not have arms-length imposed, pre-trade risk controls. The FOA believes that current definitions would benefit from further clarity, in particular with regards to the market participant controlling and implementing the risk management controls.

7.6.3 In general, if a firm is subject to, and complies with, the limits set out in Section 5.11.1 above and where such limits are imposed by a DEA Provider (where applicable), then it shall not *prima facie* be providing or taking advantage of “naked” access to a market.

7.6.4 “Arms-length” means that one or more of: (a) a Venue, (b) DEA Provider or (c) a stand-alone entity, or an entity which satisfies the independence test set out in Section 8.6, is hosting risk management infrastructure to which the DEA Provider must have sole access and control, and a non-exclusive licence.

7.7 Heart beating with Venues

7.7.1 Trading systems should be able to monitor heartbeats with the Venue to identify when connectivity to the Venue is lost. Venue cancel-on-disconnect / don’t cancel on disconnect functionality can be set either by per session/login or per trade as part of the Venue trading API.

7.8 Helpdesk policy / operations to cut-off Venue IDs or a particular entity’s trading activity

7.8.1 As a back-up of last resort, Venue helpdesk staff should be able to use the kill button / function on a Member’s behalf. The Member should provide the Venue with an authorised list of persons and identification criteria permitted to invoke this process. This list should be kept materially up to date. A Venue may retain the right to use the kill button / function unilaterally if it determines that it must use it to maintain a fair and orderly market.

7.9 Documentation of messaging and throttling policies

7.9.1 It is accepted that a Venue may not wish to publicise precise thresholds for throttling message traffic, in particular because its systems capacity is proprietary, and there is a risk that knowledge of it may be capable of being exploited in an abusive or unfair way.

7.9.2 Each Venue should make public its procedures to indicate:

(a) The types of situations in which throttling will occur;

(b) How long such throttling controls may be in place in different circumstances;

(c) The throttling values and minimum throttling value that will be applied before the market will be suspended and re-opened after a pause;

(d) That unless market participants are throttled on an individual basis, no market participant will be placed at a disadvantage *vis-a-vis* other market participants in the event that throttling occurs; and

(e) The steps the Venue intends to take to (i) rectify any event that leads to throttling controls (unless market participants are throttled on an individual basis); and (ii) penalise or censure any market participant whom it determines is at fault or contributed to the events leading to the controls.

7.9.3 Separate from a system for throttling capacity, each Venue should have the ability to pause / close markets during excessive price volatility swings or for other reasons to maintain (or re-establish) a fair and orderly, stable market.

7.9.4 Venues should have a commercial policy which disincentivises excessively high message to execution ratios.

7.10 Price collars

7.10.1 Without prejudice to any individual pre- or post-trade technical risk limits applicable to each member, each Venue should have in place functionality that oversees the prices at which orders are submitted to the market, and will either halt or constrain trading activity in accordance with pre-defined and publicly available thresholds.

7.11 Venue provides a multi-legged ATS product

7.11.1 If Venues offer a multi-legged ATS product directly to Clients, the DEA Providers:

(a) Retain the ability to switch off access to those products for some or all of their Clients at their discretion;

(b) Should, where available, be able to track orders in those products as whole strategies and not just as two or more separate orders;

(c) Should where available, be able to see working spreads as unexecuted orders on a real-time drop copy feed.

7.12 Other controls

7.12.1 Venues should provide DEA Providers and their Clients with an independent means of cancelling and amending orders (such as an internet accessible GUI).

7.12.2 In the case of a Venue-provided multi-legged ATS product, orders and their parent / child relationship should be easily identifiable as those of the relevant Member.

7.13 Post trade

7.13.1 Venues should provide drop copies of trades and orders to Members and DEA Providers (in relation to their Clients' activities) as well as to the firms clearing those trades.

7.13.2 Venues should provide DEA Providers with the ability (on request) to trigger a kill button / function for specified trading IDs in the event that drop-copy connection is lost.

7.14 Record Keeping

7.14.1 Venues should keep electronic records of the following for periods defined by their local regulatory authority:

(a) Orders and trades (including acknowledgements, fills, amendments and cancellations) in real-time; and

(b) De-activation records for inactive Venue IDs. Venues should periodically audit trading IDs. Any ID which has been inactive for at least six months should be automatically disabled pending confirmation from the Member that the Venue ID is not valid (for example, that it is not used for DRP purposes).

8. Clients' requirements of Service Providers

8.1 Service Providers are not directly regulated but may have contractual obligations to their clients derived from this Guidance.

8.2 These contractual obligations on Service Providers will depend on the services and products provided. For ease of reference, these are broken down into three areas: (a) electronic trading systems; (b) connectivity; and (c) environments or tool / development kits for use by firms in algorithm development.

8.3 For areas (a) and (b) above, the Service Provider should provide copies or summaries containing sufficient detail for its client to confirm that the Service Provider has systems, policies and procedures in place to permit the client itself to assist in maintaining a fair and orderly market, and to satisfy the clients' obligations to other market participants. For area (c), there are no specific provisions which are included in this Guidance.

8.4 Contracts with Service Providers should contain contractual protections in relation to the fitness for purpose and maintenance / updating of the products and services provided. Such contractual protections will be by way of representations, warranties and indemnities.

8.5 To the extent that Service Providers provide risk controls or management oversight functions on behalf of either the Venues or other market participants, then such controls / functions should conform to the applicable specifications set out in this document (and in particular those at Section 5.11.1)

8.6 To the extent that Service Providers provide risk controls or management oversight on behalf of either a Venue or other market participants, those controls should include automated 'restricted list' functionality where applicable to prevent trading on products that would be in breach of its compliance policy. This list should be capable of being adjusted intraday. After any adjustment, any outstanding orders for products which were not previously on a 'restricted list', and which have not been filled, should be permitted to remain on the market pending execution.

8.7 If a Service Provider offers an ATS directly to DEA Providers' Clients, the DEA Providers:

(a) Must retain the ability to switch off access to those products for some or all of their clients in at the DEA Provider's discretion;

(b) Should, where available, be able to track orders in those products as whole strategies and not just as two or more separate orders; and

(c) Should where available, be able to see working spreads as unexecuted orders on the real-time drop copy feed.

8.8 If a Service Provider is affiliated to, or spun-out from, a Member or Client, then unless Section 8.8 (a) and (b) below are satisfied, the Venues and DEA Providers shall insist (unless extraordinary circumstances prevail) that they shall be a party to any agreement with the Service Provider:

(a) There is a proper arms-length relationship between the NCM or Client and its Service Provider; and

(b) The Service Provider has real substance (including, but not limited to, substantial assets, its own management and control, and other third party, unaffiliated clients).

8.9 Contractual provisions

8.9.1 The contract with the Service Provider should include provisions and contractual protections dealing with at least the following:

(a) BCP and DRP of Service Provider;

(b) Adequacy of redundancy across Service Provider's systems;

(c) Reasonable Service Provider financial reserves to satisfy monetary obligations under contractual indemnities or warranties;

(d) Service Providers should be willing to accept escrow of code and any necessary transfer of licenses and expertise in the event of their own bankruptcy where the services provided are sufficiently material either to the Clients' own business or to financial market stability;

(e) Testing, implementation and change control procedures;

(f) Failure of systems / problems reporting;

(g) Objective service levels covering the quality and functionality of the services provided;

(h) "Chain-of-command" and complaints / escalation / out-of-hours procedure;

(i) Termination / replacement provisions;

(j) The provisions relating to termination / replacement shall ensure, so far as possible, that there will be no break in coverage for the client firm and that the client firm will be able to satisfy its obligations as regards assisting in maintaining a fair and orderly market;

(k) Provisions relating to liability of the Service Provider and restrictions on same (including the ability to seek to rely on contractual obligations and protections in dealing with counterparties and Venues); and

(l) Confidentiality and security requirements.

APPENDIX 1

APPROVAL FOR NEW STRATEGY/REVISION OF STRATEGY POLICY

NB: THIS EXAMPLE POLICY SETS OUT SOME CONSIDERATIONS AND SPECIFICS ON WHICH FIRMS SHOULD FOCUS, DEPENDING ON THEIR OWN CIRCUMSTANCES. IT IS NOT EXHAUSTIVE OR PRESCRIPTIVE IN ITS CONTENT, ISSUES OR APPROACH. FIRMS SHOULD ADAPT THIS AS PART OF THEIR OVERALL RISK MANAGEMENT POLICIES AND PROCEDURES

THIS EXAMPLE POLICY ASSUMES THAT A FIRM ADOPTING IT USES THE DEFINITIONS ETC IN THIS GUIDANCE, BUT FOR THE SAKE OF CLARITY, BREAKS DOWN A NUMBER OF POINTS INCLUDED, E.G. IN "PRE-TRADE RISK CONTROLS" INTO SPECIFIC POINTS FOR CONSIDERATION

Signed:

_____

_____

Date

ATS NAME: _____

ATS UNIQUE IDENTIFIER : _____

DESK: _____

GO-LIVE DATE: _____

Steps for Initial Approval for development of strategy or change to strategy	**Brief Description**	**Sign-Off Procedure** *(NB. No individual may sign-off for themselves)*
Team involved in strategy/strategy change		
Team business continuity arrangements (e.g. escalation of query/sign-off among team, BCP of team, specific requirements different from general firm DRP and BCP)		
Short description of strategy (in terms Venues, compliance/risk and regulator (if applicable) can understand)		
Types of order (market/limit/GTD etc.)		

Staff testing (knowledge of compliance/procedures etc.)		
Markets/Exchanges/Platforms on which strategy will place orders/trade		
Initial firm capital and other requirements to permit strategy to trade (to be discussed with CFO and confirmed with broker/GCM).		
Connectivity/API requirements (specifically, connectivity/APIs/GUIs to which firm/team does not already have access)		
Pre-trade risk controls to be applied		
Authority and process for operating a kill button / function		
Non-pre-trade risk limits or controls		
Is Venue registration required?		

Venue ID details		
Internal or other ATS or strategy identifier		

Steps for Approval of Final Implementation of Strategy/Change	**Frequency of testing (where relevant – highlighted)**	**Brief Description**	**Sign-Off** *(NB. No individual may sign-off for themselves)*
ATS strategy code testing (if applicable)			
"Market impact" considerations [Issues for teams/firms to consider depending on type of strategy, venue, asset to be traded and level of			

automation] o Trading auctions? o Participate in expiries? o Price transparency o Transaction transparency o Percentage of orders likely to be filled (e.g. depends on liquidity of market) o Time orders to remain open o Number of orders per second o Number of failed attempts at being filled o Number of successful attempts before order is changed o Max and min lot/order sizes o Trading suspension events (e.g. non-farm payroll)Market rules/participant training o Training on what constitutes market abuse for risk/trade monitoring, quants/devs and traders o Loss-limit testing o Market-movement testing o Connection-loss testing o Order send/acknowledgement receipt testing o Order receipt/order fill testing o Latency testing o Broker/connectivity testing o Settlement and counter-party			

(including own) risk			

Back-Testing and live strategy monitoring	**Frequency of testing (where relevant – highlighted)**	**Sign-Off** *(NB. No individual may sign-off for themselves)*
Connectivity testing (both internally and externally) (circuit breakers, pre-trade risk layer etc.)	**Frequency of testing:**	
Testing of arrangements for blocking, cancelling, amending or correcting transactions	**Frequency of testing:**	
Stability of correlations in back-testing to available historical data		
Data analyzed / relevant time period		

Loss limits and stop losses	**Frequency of testing:**	
Position monitoring/calculations	**Frequency of testing:**	
Market impact testing	**Frequency of testing:**	

APPENDIX 2

APPROVAL FOR TECHNOLOGY CHANGES

NB: THIS EXAMPLE POLICY SETS OUT SOME CONSIDERATIONS AND SPECIFICS ON WHICH FIRMS SHOULD FOCUS, DEPENDING ON THEIR OWN CIRCUMSTANCES. IT IS NOT EXHAUSTIVE OR PRESCRIPTIVE IN ITS CONTENT, ISSUES OR APPROACH. FIRMS SHOULD ADAPT THIS AS PART OF THEIR OVERALL RISK MANAGEMENT POLICIES AND PROCEDURES

Date:

TECHNOLOGY DESCRIPTION:

_____

RESPONSIBLE PERSON:

_____

PRIMARY REGULATORY CONTACT DETAILS:

_____

RESPONSIBLE/CONTACT PERSON FOR STAKEHOLDERS:

_____

CHANGE CHARACTERIZATION

Each change will be characterized and identified by using the definitions at the end of this policy (which will be filled-in or amended by appropriate management and experienced personnel from time to time). All changes which fall into the same category should be dealt with in the same way.

Change Type	**Responsible Person for Categorization of Change Type**	**Change Description**	**Sign-Off** *(NB. No individual may sign-off for themselves)*	

CHANGE PROCESS PROCEDURE

	Notes	**Persons Responsible**	**Sign-Off (CxO or Approved Person)**
Identification of Stakeholders			
Initiation			

Notification to Stakeholders			
Approval			
Scheduling			
Deployment: • **Preparation** • **Implementation** • **Validation** • **Completion/Reversion**			
Post-Deployment Notification to Stakeholders			
Post-Deployment Updates/Checks			

Change Types:

[1] - Minor/Technical (internal) :

[2] - Minor/Technical (externally-driven – e.g. amendment to Venue/broker API) :

[3] - Strategy-Driven (see also separate Strategy Revision Policy) :

[4] - Risk Monitoring / Management or Reconciliation-Driven :

[5] - Execution-Driven :

[6] - Connectivity-Driven (including ISVs/feed handler) :

[7] - Regulation-Driven (e.g. market abuse monitoring and reporting) :

[8] - Clearing/Broker-Driven :

APPENDIX 3

BUSINESS CONTINUITY AND DISASTER RECOVERY PROCEDURES

NB: THIS EXAMPLE POLICY SETS OUT SOME CONSIDERATIONS AND SPECIFICS ON WHICH FIRMS SHOULD FOCUS, DEPENDING ON THEIR OWN CIRCUMSTANCES. IT IS NOT EXHAUSTIVE OR PRESCRIPTIVE IN ITS CONTENT, ISSUES OR APPROACH. FIRMS SHOULD ADAPT THIS AS PART OF THEIR OVERALL RISK MANAGEMENT POLICIES AND PROCEDURES

Last updated: _____

Last DRP test date: _____

Event	**Relevant strategy (if applicable)**	**Risk (high, medium, low)**	**Potential impact (high, medium, low)**	**Actions/Mitigations**	**Responsible person(s)**
Loss of key personnel (short or medium term)					
Evacuation of building (short-term)					
Evacuation of building (long-term)/destruction of building					
Short-term disconnection with/outage of power in building					
Long-term disconnection with/outage of power in building					
Short-term disconnection with/outage of telephony system in building					
Short-term disconnection with/outage at datacenter at [where]					

Long-term disconnection with/destruction of datacenter at [where]					
Short-term disconnection with/outage at [PB]					
Long-term disconnection with/outage at [PB]					
Short-term disconnection with/outage at market/exchange/platform					
Long-term disconnection with/outage at market/exchange/platform					
Personnel changes at [PB]					
Personnel changes at datacenter at [where]					
Personnel changes at market/exchange/platform					
Deliberate or malicious user interference with code/strategies					
Deliberate or malicious user interference with equipment					
Deliberate or malicious user interference with order placing, acceptance, execution, clearing					

Deliberate or accidental third party remote access to IT/telephony systems					
Short-term disconnection of remote access to IT/telephony systems					
Long-term disconnection of remote access to IT/telephony systems					
Short-term disconnection with/Outage at market/tick data provider					
Long-term disconnection with market/tick data provider					
Difference in position reconciliation between own systems and market/exchange/platform/clearer/broker systems					

APPENDIX 4

BUSINESS SUCCESSION PLANNING

NB: THIS EXAMPLE POLICY SETS OUT SOME CONSIDERATIONS AND SPECIFICS ON WHICH FIRMS SHOULD FOCUS, DEPENDING ON THEIR OWN CIRCUMSTANCES. IT IS NOT EXHAUSTIVE OR PRESCRIPTIVE IN ITS CONTENT, ISSUES OR APPROACH. FIRMS SHOULD ADAPT THIS AS PART OF THEIR OVERALL RISK MANAGEMENT POLICIES AND PROCEDURES

Last updated: _____

Named:
Position/Title:

Main duties and responsibilities	**Other responsible persons for those duties and responsibilities**	**Steps to be taken in event Named person incapacitated to prevent lack of continuity of business**

APPENDIX 5

LIST OF FOA MEMBERS

FINANCIAL INSTITUTIONS
ABN AMRO Clearing Bank N.V.
ADMISI
Altura Markets S.A./S.V
AMT Futures Limited
Jefferies Bache Limited
Banco Santander
Bank of America Merrill Lynch
Banca IMI S.p.A.
Barclays Capital
Berkeley Futures
BGC International
BHF Aktiengesellschaft
BNP Paribas Commodity Futures
BNY Mellon Clearing International
Citadel Derivatives Group (Europe)
Citigroup
City Index
CMC Group Plc
Commerzbank AG
Crédit Agricole CIB
Credit Suisse Securities (Europe)
Deutsche Bank AG
ETX Capital
FOREX.COM UK
FXCM Securities
GFI Securities
GFT Global Markets UK Ltd
Goldman Sachs International
HSBC Bank Plc
ICAP Securities Limited
IG Group Holdings Plc
International FC Stone Group
JP Morgan Securities
Kyte Broking Limited
Liquid Capital Markets
London Capital Group
Macquarie Bank
Mako Global Derivatives
Marex Spectron
Mitsubishi UFJ Securities Int'l Plc
Mizuho Securities USA, Inc London
Monument Securities
Morgan Stanley & Co International
Newedge Group (UK Branch)
Nomura International Plc
Rabobank International
RBC Europe Limited
Saxo Bank A/S
Scotiabank Europe
S E B Futures
Schneider Trading Associates
S G London
Standard Bank Plc
Standard Chartered Bank
Starmark Trading
State Street GMBH London Branch
The Kyte Group Limited
The RBS Group
UBS Limited
Valbury Capital Ltd
Vantage Capital Markets LLP
Wells Fargo Securities

EXCHANGE/CLEARING HOUSES
APX Group
CME Group, Inc.
Dalian Commodity Exchange
European Energy Exchange AG
Global Board of Trade
ICE Futures Europe
LCH.Clearnet Group
MCX Stock Exchange
MEFF RV
Nasdaq OMX
Nord Pool Spot AS
NYSE Liffe
Powernext SA
RTS Stock Exchange
Shanghai Futures Exchange
Singapore Exchange
Singapore Mercantile Exchange
The London Metal Exchange
The South African Futures Exchange
Turquoise Global Holdings

SPECIALIST COMMODITY HOUSES
Amalgamated Metal Trading
BASF SE. EIL
Cargill Plc
ED & F Man Capital Markets
Glencore Commodities
Gunvor SA
Hunter Wise Commodities LLC
Koch Metals Trading Ltd
Metdist Trading Limited
Mitsui Bussan Commodities
Natixis Commodity Markets
Noble Clean Fuels
Phibro GMBH
J.P. Morgan Metals
Sucden Financial
Toyota Tsusho Metals
Triland Metals
Vitol SA

ENERGY COMPANIES
BP International lST
Centrica Energy
ChevronTexaco
ConocoPhillips Limited
E.ON EnergyTrading SE
EDF Energy
EDF Trading Ltd
International Power plc
Phillips 66 TS Limited
National Grid Electricity Transmission Plc
RWE Trading GMBH
Scottish Power Energy Trading
Shell International
SmartestEnergy Limited

PROFESSIONAL SERVICE COMPANIES
Ashurst LLP
ATEO Ltd
Baker & McKenzie
Berwin Leighton Paisner LLP
BDO Stoy Hayward
Clifford Chance
Clyde & Co
CMS Cameron McKenna
Deloitte
FfastFill
Fidessa Plc
Freshfields Bruckhaus Deringer
Herbert Smith LLP
Holman Fenwick Willan LLP
ION Trading Group
JLT Risk Solutions Ltd
Katten Muchin Rosenman LLP
Linklaters LLP
Kinetic Partners LLP
KPMG
McDermott Will & Emery LLP
Mpac Consultancy LLP
Norton Rose LLP
Options Industry Council
Orrick, Herrington & Sutcliffe LLP
PA Consulting Group
R3D Systems Ltd
Reed Smith LLP
Rostron Parry
RTS Realtime Systems
Sidley Austin LLP
Simmons & Simmons
SJ Berwin & Company
SmartStream Technologies
SNR Denton UK LLP
Speechly Bircham LLP
Stellar Trading Systems
SunGard Futures Systems
Swiss FOA
Trading Technologies
Traiana Inc
Travers Smith LLP
Trayport