FIA Due Diligence Questionnaire for IT outsourcing and procurement

[MIFID II, RTS 6, Article 4 specifies "an investment firm shall remain fully responsible for its obligations under this regulation where it outsources or procures software or hardware used in algorithmic trading activities."

In practice this means that many market participants will approach the same set of vendors with the same set of questions expressed in different ways. In order to prevent nugatory work, the FIA have produced a Vendor Due Diligence Questionnaire. The purpose of this document is to provide a standard form for firms to request information so as to allow a vendor to communicate MIFID II conformance to many customers through a single document.

The terms Algorithmic trading and DEA are assumed to be as defined by MIFID II below.

Algorithmic trading: *trading in financial instruments where a computer algorithm automatically determines individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission, with limited or no human intervention, and does not include any system that is only used for the purpose of routing orders to one or more trading venues or for the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions*.

Direct Electronic Access (DEA): *an arrangement where a member or participant or client of a trading venue permits a person to use its trading code so the person can electronically transmit orders relating to a financial instrument directly to the trading venue and includes arrangements which involve the use by a person of the infrastructure of the member or participant or client, or any connecting system provided by the member or participant or client, to transmit the orders and arrangements where such an infrastructure is not used by a person.]*

Disclaimer

This document is provided for the benefit of FIA members and is for informational purposes only. Although care has been taken to assure that the content is accurate as of the date of publication, this document is not intended to constitute legal or regulatory advice. FIA specifically disclaims any legal responsibility for any errors or omissions and disclaims any liability for losses or damages incurred through the use of the information herein. FIA undertakes no obligations to update this document following the date of publication.

Questionnaire

Vendor Name:

Name and contact details of the person completing form:

Introduction and overview

1.1 Overview of activities of the vendor

1.2 Key financial information (for example but not limited to p&l, balance sheet) of the vendor

1.3 Description of your services/products

1.4 Description of services provided to the customer

1.5 Provide a list of algorithms provided to the customer and explain how they work

1.6 Organisation chart

1.7 Description of your enquiry/complaint/order process escalation

1.8 Up-to-date contact information for relevant personnel

1.9 Description of changes to responses since last response

General Organisational Requirements

2.1 Explain the procedures you use to approve the development, deployment and subsequent update of trading algorithms [RT6, Article 1].

2.2 Explain how information should be passed to/from your customers. In particular, information about releases to customers and information about issues from customers [Article 1].

2.3 How do you train staff trained in the compliance/regulatory obligations relevant to the system? [Article 3]

2.4 Please list all material services for which you rely on third parties, consultants and/or outsourced providers (including data storage facilities for your records) which are relevant to the products and services you provide to the customer. [Article 4]

Resilience: Testing and Deployment

3.1 Explain your development and testing processes [Article 5.1]

3.2 Describe your authorisation process before a new release. Do you allow your customers to test releases and approve them before they implement them? [Article 5.2]

3.3 What records are kept of evidence that the design, development, testing and release processes have been followed? How long are they kept for? [Article 5.3]

3.4 How do you ensure that the products and services you provide comply with the rules of trading venues and other relevant regulation? [Article 5.5]

3.5 How do you ensure that the products and services you provide will not contribute to disorderly trading and will continue to function in stressed market conditions? [Article 5.4]

3.6 How do you support customers in testing to trading venues? How is this also applied for changes to algorithmic trading products and services? [Article 5.4]

3.7 Explain how and for how long you retain records for material changes, specifically covering when the change was made, the person that made it, the person that approved it and the nature of the change. [Article 5.7]

3.8 Under what circumstances do you carry out conformance testing with an exchange? How do you do this? How do you define a "material change"? [Article 6]

3.9 (If you run a separate production environment) How do you separate production and testing environments? Do you ever test a product or service in a production environment? [Article 7]

3.10 What facilities do you provide to allow your customers to restrict use of a product or service when it is deployed?

3.11 Does you system have self-match protection? Explain how it works?

Resilience: Post-deployment management

4.1 With what frequency do you review your development process? Explain how the review is carried out and the output reviewed/actioned. [Article 9]

4.2 What stress testing do you carry out on your product? How do you define the volume that you use to stress the products and services? [Article 10]

Resilience: Means to ensure Resilience

5.1 What "Kill Functionality" do you provide to assist customers to cancel any or all unexecuted orders submitted to any or all trading venues? [Article 12]

5.2 How can a customer identify which trading algorithm and which trader is responsible for an order? [Article 12.3]

5.3 What functionality do you provide to assist with monitoring of trading and automated surveillance? [Article 13]

5.4 (If providing a service) Describe your business continuity arrangements. In particular, the governance framework, an overview of the relocation procedures, staff training, arrangements for shutting down the products or services and any alternative arrangements. [Article 14]

5.5 What pre-trade controls do your products and services apply to flow classified as DEA by your customers? In particular price controls, max order values/volumes, message limits and position controls. [Article 15]

5.6 What controls are applied by the products or services to algorithms? In particular price controls, max order values/volumes, message limits, position controls and the number of times an algorithm has been applied? [Article 15]

5.7 What facilities do your products or services provide for real time monitoring of algorithmic trading? How can this be permissioned for an independent risk function that should not have trading access? [Article 16]

5.8 What facilities do you offer to help customers with continuous assessment of market and credit risk? [Article 17]

5.9 How do you reconcile open orders in the system with open orders in the market in real time? [Article 17.3]

5.10 Explain how your max long/short and overall strategy positions are managed. [Article 17.4]

5.11 Outline your security policy and how it is implemented in your organisation. [Article 18]

5.12 In the event security measures are compromised, explain how you will know and how you will communicate this. [Article 18.3]

5.13 Explain how penetration tests and vulnerability scans are carried out and give the frequency with which you carry out this testing. [Article 18.4]

5.14 How do your products or services control persons who have critical access rights? How is this monitored? Include in the answer those with system administration rights and data administration rights. [Article 18.5]

5.15 Who in your company or at external companies providing services/products has access to data entered by customers? What steps do you take to protect customer confidentiality? [Article 18.5]

Order Record Keeping

6.1 Will you provide data extracts covering a superset of the general order record keeping requirements under MiFID II and the ones for investment firm that engages in a high-frequency algorithmic trading technique, regardless of how the vendors customers are categorised? [RTS6, annex]

6.2 What means are available within your services and products to manage the ratio of unexecuted orders to transactions?

6.3 What measures are in place to ensure privacy of client, order and trade data? [Article 2.3]

6.4 Certain fields are sent by the trading venue when confirming an execution. Examples include: Waiver Flag, Routing Strategy, Liquidity Indicator. How do you intend to handle these values?

6.5 Describe your clock synchronisation solution (RTS25).

Best Execution

MIFIDII expects Investment Firms to deliver Best Execution by having Best Execution policies, following them and monitoring their utility. Outsourcing processes and services to vendors means outsourcing some of the ways that Best Execution is achieved but does not negate the need of Investment Firms to monitor.

7.1 How do you ensure Best Execution within your services and systems?

7.2 Explain how you monitor and review this? What evidence do you retain?

7.3 What framework do you have for monitoring service quality / software issues with your customers?

7.4 What functionality do you provide that help you customers monitor execution quality?