MANAGED NETWORKS

Managed Networks' guide to MiFID

Ben Rapp, CEO

June 2007

Table of Contents

Table of Contents 2

Introduction 3

About MiFID 4

- So what exactly is MiFID? 4
- Whom will it affect? 4
- When is this happening? 4
- Why is this relevant to IT? 4

MiFID compliant outsourcing 6

- How do we make our contracts MiFID compliant? 6
- List of contract requirements 6

Benefiting from MiFID 9

- So how is this an opportunity to gain business advantage? 9
- Useful services and products 9

Conclusion 12

Further reading 13

Disclaimer 14

Introduction

This paper is designed to offer advice and ways forward for IT managers and compliance officers in firms which are affected by the implementation of the Markets in Financial Instruments Directive (MiFID). It does not explain MiFID completely, but looks to:

- Give a brief overview on what MiFID is, what it is trying to do, and who it affects
- Explain why clients should be thinking about MiFID in the context of their IT.
- Discuss the requirements now placed on outsourcing arrangements, offering an view on what the regulations mean for outsourced service arrangements in practice
- Provide an insight into how MiFID can be an opportunity for regulated firms to gain a commercial advantage over their competition by implementing the best practices that are encapsulated in the MiFID regulation and guidance.

For those who require further information and guidance on MiFID, further reading is suggested at the end of the paper.

About MiFID

So what exactly is MiFID?

It stands for the **M**arkets **i**n **F**inancial **I**nstruments **D**irective. It is a European Union initiative to create a harmonised regulatory regime for the provision of a variety of financial services and their markets in Europe.

The key elements of MiFID are:

1. Investment firms will, on the basis of their home country authorisation be able to provide investment services throughout the EU. This is called "passporting" when the firm is trading outside its home market. MiFID also clearly apportions the responsibility between home state and host state for passporting investment firms.
2. MiFID is designed to create a level playing field for firms by harmonising the authorisation and ongoing regulatory requirements for different types of investment firms; it is expected that this will encourage competition between firms.
3. MIFID incorporates significant protections for investors, by harmonising the conduct of business rules with which investment firms have to comply. The old Investment Services Directive, which MIFID replaces, was being undermined by member states imposing different conduct of business rules in their particular territories.
4. MIFID increases and deepens the organisational responsibilities for affected firms, including the specific regulation of outsourcing and business continuity provision.

Whom will it affect?

MIFID will impact the activities of retail banks; investment banks; portfolio managers (collective investment scheme fund managers will be caught in part); stockbrokers and broker dealers; many futures and options firms; corporate finance firms; wholesale market brokers; operators of regulated markets (RMs) and multilateral trade facilities (MTFs); providers of custody services; and some commodities and venture capital firms.

The FSA has also extended the application of MIFID organisational requirements to what they term as common platform firms; these are firms that are subject to the Capital Requirements Directive (CRD). This was done because the FSA felt that most firms subject to the CRD were also subject (at least in part) to MiFID, and it would be tidier to have unified regulatory principles. This means, however, that some firms who are not subject to MiFID will nonetheless have to make some of the organisational changes required by MiFID; insurers are an example.

When is this happening?

1 November 2007 is the date on which all the MiFID-related implementing legislation will have effect. Member States were required to have finalised their implementing legislation since last January. It remains to be seen whether all Member States will be organised by the 1 November deadline.

Why is this relevant to IT?

Two reasons:

1) If you outsource any business-critical services to FSA-regulated customers, and are subject to MiFID regulation, then your relationship with your outsourced service provider is directly regulated for the first time. You need to read the notes

on key MiFID outsourcing requirements that follow in this document, and make sure that all of your outsourcing contracts are compliant before 1 November.

2) MiFID affects a wide range of your internal processes, procedures and controls. Your supplier will need to ensure that the products and services they provide allow you to be compliant with the new regulations. By the same token, they may be able to offer new services or products that assist you with compliance and provide a business advantage.

MiFID compliant outsourcing

How do we make our contracts MiFID compliant?

There are a number of requirements affecting IT service provision resulting from MiFID; some of these will need to be written into your contracts and service level agreements (SLAs), others may require your supplier to change the way your service is delivered. It is important to remember that these requirements only apply to the service if it is deemed to be outsourcing of a critical business activity. The outsourced activity would be seen as a business critical activity if the regulated firm would be prevented from carrying out its business, serving its clients or complying with regulation by the failure of the service.

List of contract requirements

The following section discusses the regulatory requirements regarding outsourcing (*in italics*), and offers guidance to members on what these mean to them and how to comply.

The requirements discussed here can be found in the FSA Handbook, section SYSC 8.1, which can be found here: http://fsahandbook.info/FSA/html/handbook/SYSC/8/1

1. *The service provider must have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally.*

   For IT companies, we take this to mean that:

   1. They must demonstrate that they have enough staff and technical resource to deliver their service even in the event of a reasonable amount of unplanned absence or systems failure. This must include a business continuity plan.
   2. They must make sure that their own business is compliant with the regulation that affects it. Unless there is specific regulation for their business area, this predominantly means general business legislation, such as planning controls, health and safety and so forth. It may be that the regulated firm will be required to demonstrate that they have checked their IT supplier's compliance with these regulations, so the IT supplier should ensure that this is the case.
   3. It may also be sensible for IT firms to obtain vendor or industry certifications as a way of demonstrating a commitment to professionalism and providing independent assurance.

2. *The service provider must carry out the outsourced services effectively, and to this end, the firm must establish methods for assessing the standard of performance of the service provider.*

   You must ensure that your contractual arrangement with the supplier includes metrics-based assessment of performance, and that they are able to provide regular reporting of these metrics.

3. *The service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing.*

   You should include regular service review meetings and service performance reports in your agreement with the supplier; you should also ensure that any proposed changes or additions include a risk assessment as part of the project workflow.

4. *Appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements.*

   Clear performance warranties and dispute resolution procedures built into your agreement with the supplier will allow you to have some influence over how matters proceed if there is a problem with the service. This is primarily an obligation on the regulated firm.

5. *The firm must retain the necessary expertise to supervise the outsourced functions effectively and manage the risks associated with the outsourcing.*

   As above, this is primarily your responsibility as the regulated firm, but you should require your supplier to provide documentation and training material that you can use to improve your management of their service provision.

6. *The service provider must disclose to the firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements.*

   The FSA has no powers to regulate service providers. By implication, therefore, the responsibility for ensuring that this disclosure takes place falls on the regulated firm. You must therefore ensure that a suitable requirement to disclose forms part of your contract with the supplier.

7. *The firm must be able to terminate the arrangement for the outsourcing where necessary, without detriment to the continuity and quality of its provision of services to clients.*

   You may need to review the termination provisions in your contracts. It is unclear what 'necessary' may mean; you must assume, we think, that you must be able to terminate the contract at any time, without fault, subject to reasonable notice and loss of profit provisions, and that the supplier must agree to provide assistance with the handover of responsibilities for the services they are providing.

8. *The service provider must co-operate with the FSA and any other relevant competent authority in connection with the outsourced activities.*

   As with 6, this appears to place a significant burden of direct regulation on the service provider. Since no obvious means of direct compulsion would be available, it becomes a responsibility of the regulated firm. Your confidentiality agreements and other relevant aspects of your contracts should be amended to reflect this requirement and require the supplier's compliance.

9. *The firm, its auditors, the FSA, and any other relevant competent authority must have effective access to data related to the outsourced activities, as well as to the business premises of the service provider and the FSA and any other relevant competent authority must be able to exercise those rights of access.*

   To be compliant, you will need your supplier to include provisions for access to information and premises for all the relevant parties (you, your auditors, the FSA and any other relevant regulators) in your outsourcing agreement. Our present opinion is that this regulation does not establish a *prima facie* right of access to the outsourcer's premises and information without initial recourse to the client regulated firm.

10. *The service provider must protect any confidential information relating to the firm and its clients.*

It seems unlikely that this will have any impact, as your existing contracts will contain confidentiality provisions or be subject to over-riding non-disclosure agreements. If this is not the case, you will need to revise your contracts accordingly.

11. *The firm and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities where that is necessary having regard to the function, service or activity that has been outsourced.*

    This requirement is an opportunity to drive the necessary change in your organisation as well as a burden. In addition, if the supplier does not have a business continuity plan for their own organisation, they must now at least have one for any service that they are providing that falls under these regulations. You will need to ensure that they can demonstrate that it is documented and tested, and that the documentation and test results are available to you so that you can show them to the FSA if required. By the same token, you should require your supplier's assistance in formulating and executing your own business continuity plan.

12. *The firm must ensure that the respective rights and obligations of the firm and of the service provider are clearly allocated and set out in a written agreement.*

    If you don't have a contract for the services you are receiving, get one. Make sure your contract (new or existing) accounts for all of the provisions listed here, which can be found in the FSA Handbook.

13. *A firm should notify the FSA when it intends to rely on a third party for the performance of operational functions which are critical or important for the performance of relevant services and activities on a continuous and satisfactory basis.*

    This requirement mainly affects you; however, you should expect your supplier to assist you with your understanding of which of the services they are providing may be included in this regulation.

Benefiting from MiFID

So how is this an opportunity to gain business advantage?

MiFID will affect a number of systems and processes, and in many cases firms (particularly small and tiny firms) have not yet fully assessed how MiFID will impact them – much less begun planning for how they will be compliant with the new requirements. Acting now to meet the MiFID requirements will give you a first-mover advantage.

You will also find that many of the requirements of MiFID, and of FSA regulation in general, are based on sensible best practice. MiFID may be the lever needed to convince all of the stakeholders in your firm that they should implement processes and systems that you believe will benefit the business.

Useful services and products

Below is a list of a few of the types of products and services that firms might require in order to become MiFID-compliant. These are followed by the specific areas of MiFID that these apply to and the relevant FSA Handbook sections.

Two-factor authentication

This type of product can help firms to be compliant with their obligations under conflicts of interest and record keeping, as audit trails will be required to identify individual behaviour.

MiFID: Conflicts of interest: Articles 13(3), 13(6), 13(9), 18, 19(7), 21(5) 25(2) and arts 21-25 of the level 2 directive.

Record keeping: 13(6), 13(9), 19(7), 21(5) 25(2) and in arts 12(2)(b) second par and (c), 16(1)(a)(b), 23 and 51 of the level 2 directive and in arts 7.8 and 24 of the level 2 regulation.

FSA: SYSC 9; SYSC Schedule 1; COB 7.1; COB 7.12; COB Schedule 1; MAR Schedule 1

Encryption

This type of product can provide a competitive advantage in comparison to other NOMADS/advisers/brokers by demonstrating commitment to client confidentiality.

MiFID: Articles 13(2)-13(8). The most direct client confidentiality obligation is in art 5(2) of the level 2 directive; see also art 12 of the level 2 regulation (reporting channels).

FSA: SYSC 4.1; SYSC 13.7.7

Email archiving

Record-keeping requirements include emails, and will also require effective search and retrieval tools for information to be retrieved in a timely fashion.

MiFID: The record keeping requirements are in articles 13(6), 13(9), 19(7), 21(5), 25(2) and in arts 12(2)(b) second par and (c), 16(1)(a)(b), 23 and 51 of the level 2 directive and in arts 7, 8 and 24 of the level 2 regulation.

FSA: SYSC 9; SYSC Schedule 1; COB 7.12; COB Schedule 1; MAR Schedule 1

Perimeter defence and logging

MiFID-specific benefits include the tracking of external website visits, and logging inbound e-mails, which negates deletion by the user. MiFID obligations around client confidentiality and conflicts of interest are relevant to this.

MiFID: Conflicts of interest: Articles 13(3), 18 and arts 21-25 of the level 2 directive

Client confidentiality: Art 5(2) of the level 2 directive

FSA: SYSC 4.1; SYSC 5.1; SYSC 10; SYSC 13.7.7; COB 7.1

CRM software

In addition to obvious general benefits, the specific application is for compliance with Principles 6 and 8, specifically with regard to conflicts of interest. Without a good CRM system it can be difficult, especially in large or geographically distributed firms, to know whether one is dealing with the same party for two conflicting purposes.

MiFID: Articles 13(3) 13(6), 13(9), 18, 19(7), 21(5) 25(2) and arts 21-25 of the level 2 directive

FSA: PRIN 2.1 (6 & 8); SYSC 5.1; SYSC 10; COB 7.1

Document management (DM) systems and other collaboration systems

There are important obligations regarding record keeping under MiFID that DM can address; further, it can also work with CRM solutions to support conflict of interest prevention and ensure the integrity of information contained in documents through audit trails and version control.

MiFID: Articles 13(3), 13(6), 13(9), 18, 19(7), 21(5) 25(2)

FSA: SYSC 5.1; SYSC 9; SYSC 10; SYSC Schedule 1; COB 7.1; COB 7.12; COB Schedule 1; MAR Schedule 1

Business continuity and disaster recovery provision

There are new requirements on business continuity, which are much more than simply having a back up. In outsourcing arrangements particularly, joint business continuity plans must be created and rehearsed where appropriate.

MiFID: Article 13(4); see also 5(3) of the level 2 directive

FSA: SYSC 4.1.6-8

MiFID-compliant outsourcing of IT functions

As discussed above, this activity is now heavily regulated. You must be compliant with MiFID to be able to act as an outsourced service provider to a regulated firm.

MiFID: Article 13(5); also see Arts 12(2)(b) second par and (c) and arts 13,14 and 15 of the level 2 directive

FSA: SYSC 8; SYSC 13.9

Telephone recording systems and unified messaging

Telephone recording will become a part of record keeping requirements, especially around taking orders to trade. Recording of both inbound and outbound calls will assist firms with complying with record keeping and proving fair dealing with clients.

MiFID: Articles 13(6), 13(9), 19(7), 21(5), 25(2), 12(2)(b) second par and (c), 16(1)(a) and (b), 23 and 51 of the level 2 directive, and arts 7,8 and 24 of the level 2 regulation

FSA: SYSC 9; SYSC Schedule 1; COB 7.12; COB Schedule 1; MAR Schedule 1

Electronic reporting and in the future, XBRL readiness

Electronic reporting to regulators will be mandated (subject to exceptions), and there are requirements on the information that must be reported.

MiFID: Articles 25 and art 12s and 13 of the level 2 regulation

FSA: SUP 16; SUP 17

Data Quality investigation

Firms will need to check their data, as requirements under client classification and know your customer mean extra, and accurate, information must be known about your clients. This will also affect a firm's conflicts of interest policy.

MiFID: Articles 13(3), 18, 19(4), 19(7), 21(5), 24; 28 and 50 level 2 directive

FSA: SYSC 5.1; SYSC 10; COB 4.1; COB 5.2; COB 7.1

Risk Governance

Risk management packages will assist with new obligations around risk management and reporting to senior management.

MiFID: Articles 13(2), 13(5); see also art 7 level 2 directive

FSA: SYSC 6; SYSC 7; SYSC 11; SYSC 12; SYSC 13; SYSC 14; SYSC 15; SYSC 16; SYSC 17

Process mapping and management.

Firms, especially those operating in more than one country, will need to ensure that everyone understands and is aware of company processes that are now more explicitly regulated by MiFID, such as resolving conflicts of interest and the firm's best execution practice.

MiFID: Articles 13(3), 14(3), 18, 19(1), 21

FSA: SYSC 5.1; SYSC 10; COB 7.1; COB 7.5; COB 7.6; COB 10.5

Trading Platforms

These will be affected by the new requirements around pre- and post- trade transparency.

MiFID: Articles 27(3), 28(1), 29(1), 44(1), 45(1)

MTFs Rec (6) (49), (56), 4(1)(15), 13, 14, 26, 34 and 35

RMs Rec (6) (49), 33,34,39,40, 41, 42 and 43

SIs Arts 4(1)(6). 4(1)(7) and art 27 and arts 21-26 of the level 2 regulation.

FSA: MAR 5.7; MAR 5.8; MAR 5.9; MAR 6.5; MAR 7

Order Management Systems

Order management systems will now need to consider the record keeping obligations relating to MiFID. These obligations relate not only to the retention of the data, but also to the retrieval, as it must be accessible in a timely manner.

MiFID: Articles 13(6), 13(9), 19(7), 21(5), 25(2)

FSA: SYSC 9; SYSC Schedule 1; COB 7.12; COB Schedule 1; MAR Schedule 1

Clearing Platforms

Again, these systems will need to consider firms' obligations around record keeping and pre- and post- trade transparency; these will also be affected by the reporting requirements.

MiFID: Articles 13(6), 13(9), 19(7), 21(5), 25(2), 27, 28(1), 29(1), 44(1), 45(1)

FSA: SYSC 9; SYSC Schedule 1; COB 7.12; COB Schedule 1; MAR 5.7; MAR 5.8; MAR 5.9; MAR 6.5; MAR 7; MAR Schedule 1

Conclusion

This document is designed to give clients a brief overview of MiFID, how it well affect you (with particular regard to your outsourcing arrangements), and how you can see MiFID as a business opportunity. MiFID is a significant issue, and opportunity, for regulated firms, and we believe will continue to be up to (and indeed beyond) the 1 November deadline.

Those clients seeking further information about MiFID and relevant guidance should make use of the further reading section at the end of the paper.

Further reading

FSA Handbook:

http://fsahandbook.info/FSA/index.jsp

FSA Discussion paper on Industry Guidance:
http://www.fsa.gov.uk/pages/library/policy/dp/2006/06_05.shtml

Christina Sinclair (FSA) explains the Common Platform approach:

http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2006/0515_cs.shtml

FSA Summary of the CRD:

http://www.fsa.gov.uk/pages/About/What/International/basel/pdf/crd_categories.pdf

MiFID Connect Outsourcing Guidance:

http://mifidconnect.com/content/1/c4/92/35/MiFID_Connect_Outsourcing_Guide.pdf

Disclaimer

This paper has not been reviewed by the FSA; it must therefore be considered to be in draft form. It represents the views of its authors and Managed Networks. We intend to submit it to the FSA for review in the hope of achieving 'FSA confirmation' in due course.

References in this document to external sources are indicative only. Managed Networks makes no warranty as to the accuracy of external documentation and has no responsibility for it. While Managed Networks has made every effort to ensure that references are accurate and complete, this is not guaranteed. References to the FSA handbook were compiled on 06 June 2007; the referenced sections may have been changed or deleted and additional sections may have been added. Before acting on any of the information in this document members are advised to seek clarification from the FSA.

MANAGED NETWORKS

North

The Heath Business Park

Runcorn WA7 4QX

Midlands

111 Hagley Road, Edgbaston
Birmingham B16 8LB

South East

6-8 Bonhill Street

London EC2A 4BX

For more information call us free on

0800 783 6170