Midmar Capital

Compliance Manual

Version number 20

August 2022

Compliance Undertaking

All new staff members, Approved Persons and staff members within scope of SM&CR of Midmar Capital LLP (the Firm) are required to read this Compliance Manual and must then acknowledge having understood it by entering their name, signing and dating this page and returning it to the Firm.

I confirm receipt of the Firm's Compliance Manual and associated Appendices (the Manual) and I hereby undertake:

1. To conform with the rules and regulations of the Financial Conduct Authority (FCA) as if such rules and regulations were directly binding on me, insofar as it is reasonably in my power to do.
2. To comply and co-operate fully with all the instructions, directions, requirements or requests properly made or imposed by or on behalf of FCA, including, but not limited to, a requirement to make myself readily available and truthfully to answer all questions put to me in the course of an inspection, investigation or any process or proceeding under the supervision or enforcement chapters of the FCA's Handbook.
3. To observe and comply with all of the Firm's financial crime and money laundering procedures which are set out in the Firm's Manual and as they may be amended from time to time.
4. To familiarise myself with, and at all times comply with, the principles, standards, requirements and procedures set out in this Manual and, in case of doubt as to the application of the Manual, to consult the Compliance Officer.
5. To observe the Market Abuse Regulation and Part V of the Criminal Justice Act 1993, in its present form and as it may be amended or replaced in future, and the requirements regarding personal account transactions that are set out in the Manual.
6. To observe the UK Bribery Act 2010 in its present form and as it may be amended or replaced in future, and the requirements regarding inducements and conflicts of interest that are set out in the Manual.
7. To observe the Money Laundering Regulations 2017 and Criminal Finances Act 2017 in their present forms and as they may be amended or replaced in future, and wider financial crime requirements set out in the Manual.

I agree that this undertaking extends to any amended or replacement requirements that you set out in any written notice which you subsequently give to me on this subject.

Where relevant, as an Approved Person under the Approved Persons Regime or Senior Managers and Certification Regime, I can confirm that I have read and will comply with the FCA's Statements of Principle for Approved Persons or the FCA's Conduct Rules, as applicable.

I understand and acknowledge that breaches of the above undertaking may be treated as serious misconduct justifying summary dismissal, AR termination, and/or withdrawal of approval.

Name

Signed

Date

Contents

1 INTRODUCTION

1.1 Purpose

This Compliance Manual and associated Appendices (the Manual) is provided to all members of staff and Appointed Representatives (ARs) upon joining the Firm. It is essential that they **read and familiarise themselves with the various chapters of the Manual and abide by it**.

1.2 Regulatory Context

Regulation of financial services in the UK is split between 2 regulatory bodies and from 1 April 2013 replaced the previous structure of one regulator of the Financial Services Authority (FSA). Under 'twin peaks' regulation, prudential supervision of large financial institutions including banks etc is carried out by a body called the Prudential Regulation Authority (PRA), and prudential supervision of all other entities including smaller investment firms, and also conduct of business of all authorised entities (including PRA authorised entities) is carried out by the Financial Conduct Authority (FCA).

The Firm is authorised and regulated by the FCA under the Financial Services and Markets Act 2000 (FSMA). Its firm reference number (FRN) is **519772**.

The FCA has the single strategic objective of protecting and enhancing confidence in the UK financial system and 3 operational objectives:

- Securing an appropriate degree of protection for consumers.
- Promoting efficiency and choice in the market for financial services.
- Protecting and enhancing the integrity of the UK financial system.

Under the FCA's supervision regime, the Firm has been considered a 'flexible portfolio' firm. This is perceived as a lower risk category of supervision compared to 'fixed portfolio' firms which have more intense supervision.

This Manual reflects the Firm's regulation by the FCA and does not reflect any requirements of the PRA unless otherwise specified.

UK regulated activities are defined under FSMA by the Regulated Activities Order (RAO) 2001, and also in the EU by the Markets in Financial Instruments Directive (MiFID), first implemented in November 2007 (MiFID 1) and updated in January 2018 (MiFID II). The regulations determine the type of regulated activities that a firm can provide under its scope of permission as detailed in section 1.5 of the Manual. They also define the rules that a firm must follow. This includes for firms called 'common platform' firms which are firms covered by both MiFID and the EU Capital Requirements Directives (CRD 1-4). The Firm is a common platform firm.

From 22 July 2013, the EU Alternative Investment Fund Managers Directive (AIFMD) was implemented in the UK and the EU. This introduced a new regulated activity of managing an unregulated collective investment vehicle which is defined as an alternative investment fund (AIF). From that date, the Firm also has permission to manage an AIF and is deemed to be a small authorised (sub-threshold) AIF. This means it is only permitted to act as an AIF for aggregate funds under management of €100m or, where certain conditions relating to leverage and redemptions are met by all funds under management, a higher aggregate limit of €500m.

At 11pm on 31 December 2020, the transition period that followed Brexit on 31 January 2020 ended, meaning that the UK was no longer a member of the EU and was no longer subject to EU legislation. Where

relevant, existing EU legislation was 'onshored' and, for example, the above MiFID and AIFMD regulations became 'UK MiFID' and 'UK AIFMD' respectively.

1.3 FCA General Principles

There are **11 Principles** and they are a general statement of the fundamental obligations of all firms under the regulatory system. In substance, the Principles express the main dimensions of the 'fit and proper' standard set for regulated firms. Being ready, willing and organised to comply with the relevant rules and requirements is therefore a critical factor and may call into question whether the Firm is still fit and proper.

The Principles are also designed as a general statement of the regulatory requirements in new or unforeseen situations and in situations in which there are no specific rules or guidance.

1. **Integrity** – a firm must conduct its business with integrity.
2. **Skill, Care and Diligence** – a firm must conduct its business with due skill, care and diligence.
3. **Management and Control** – a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
4. **Financial Prudence** – a firm must maintain adequate financial resources.
5. **Market Conduct** – a firm must observe proper standards of market conduct.
6. **Clients' Interests** – a firm must pay due regard to the interest of its clients and treat them fairly.
7. **Communications with Clients** – a firm must pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair and not misleading.
8. **Conflicts of Interest** – a firm must manage conflicts of interest fairly, both between itself and its clients, and between one client and another.
9. **Client Relationships of Trust** – a firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any client who is entitled to rely on its judgement.
10. **Client Assets** – a firm must arrange adequate protection for its clients' assets when it is responsible for them.
11. **Relations with Regulators** – a firm must deal with its regulators in an open and co-operative way and must disclose to the FCA appropriately anything relating to the firm of which the FCA would reasonably expect prompt notice.

The FCA has a detailed Handbook of rules and guidance, setting out exactly how the Firm and its ARs should carry out its business, and with which it must comply. This Manual contains the procedures that will enable the Firm and its ARs to be compliant with various regulatory requirements to which it is subject.

The Manual does not replace or attempt to replicate the FCA Handbook, which, as mentioned above, has explicit application to the Firm according to its status under relevant regulations. The Manual makes frequent reference to the FCA Handbook in order to direct the user, when an issue arises, back to the source of rules and regulations for further clarification. The FCA Handbook can be found on the FCA's website.

1.4 The Compliance Officer

Gillian Gallacher is the Firm's Compliance Officer. Staff members with any queries or concerns in respect of regulatory matters or compliance issues, should consult the Compliance Officer, failing which another partner or alternatively Emma Jones as Deputy Compliance Officer.

The Compliance Officer is responsible for ensuring that the Manual is kept up to date and abreast of any new or amended rules or regulations. **Should staff members be in doubt about the application of any rules, whether it is imposed by the Firm or necessary under the FCA's rules, they should consult the**

Compliance Officer immediately. The Firm will treat any instances of non-compliance very seriously and this can ultimately lead to the dismissal of members of staff or withdrawal of an individual's FCA approval (where relevant).

1.5 FCA Authorisation and Approval

The FCA's Scope of Permission Notice (SOPN) (see below) sets out the regulated activities that the Firm is authorised to conduct, together with the specific investments in relation to those specific activities. The SOPN will also set out the type of clients that the Firm can deal with (Professional Clients and Eligible Counterparties). It will also set out any limitations to which the Firm is subject. **It is essential that if anyone is unclear as to whether they are permitted to carry out a particular activity, they must consult the Compliance Officer prior to carrying out that activity**.

The Firm's Scope of Permission

The Firm is currently authorised as a MiFID investment manager and a sub-threshold alternative investment fund manager with the following scope of permission:

- Dealing in investments as agent.
- Arranging (bringing about) deals in investments.
- Making arrangements with a view to transactions in investments.
- Advising on investments (except pension transfers and pension opt-outs).
- Establishing, operating or winding up a collective investment scheme.
- Managing an unauthorised AIF.
- Managing investments.
- Agreeing to carry on a regulated activity (within the Firm's scope of permission).

The Firm can undertake these activities in relation to the following client types:

- Eligible Counterparties.
- Professional Clients.

The Firm can undertake these activities in relation to the following specified investments:

- Certificates representing certain security.
- Commodity future.
- Commodity option and option on commodity future.
- Contract for differences (excluding a spread bet and a rolling spot forex contract).
- Debenture.
- Future (excluding a commodity future and a rolling spot forex contract).
- Government and public security.
- Option (excluding a commodity option and an option on a commodity future).
- Rights to or interests in investments (contractually based investments).
- Rights to or interests in investments (security).
- Rolling spot forex contract.
- Share.
- Unit.
- Warrant.

The Firm is **NOT** permitted to:

- Act for Retail Clients.
- Hold client money or assets.

- Deal as principal.

Due to Brexit, from 31 December 2020, the Firm does not currently have permission to provide regulated investment activities in any country outside of the UK. As part of automatic Brexit transition, it does have a MiFID passport for certain services in Gibraltar but at present has not exercised these rights. Otherwise, should the Firm's geographical scope change, unless some form of 'equivalence' agreement formally exists between the UK and a relevant country, it is anticipated that the Firm would need to become directly regulated in the non-UK country in question. This includes EU member states and the US.

1.5.1 Appointed Representatives

From time to time, the Firm may have arrangements in place with other legal entities for such firms to be ARs of the Firm. Such firms are not authorised firms under the FSMA. However, they are exempt from authorisation where an authorised firm takes responsibility for their actions and omissions. The authorised firm is deemed to be the principal under such an arrangement.

For the avoidance of doubt, this Manual applies to each and every AR of the Firm and also any member of staff (whether permanent or temporary) and anyone acting on behalf of that AR. The Firm has a documented AR contract in place with any such entities which outlines roles and responsibilities, obligations and duties. Any AR must always act within this agreement and also within the Firm's own scope of permission otherwise it will breach the provisions of the FSMA and incur potential sanctions on both the AR and the principal (i.e. the Firm).

In relation to regulated activities, the type of activities an AR can carry out under its arrangement with the Firm include advising on and arranging deals in investments. However, it **excludes** managing investments (including an AIF) as this is not a permitted activity under the Appointed Representative Regulations.

No firm can act as an AR of the Firm until it has been added to the FCA register entry for the Firm. An application for such approval (along with the Approved Person applications for relevant AR staff) by the FCA will be submitted by or on behalf of the Compliance Officer following appropriate due diligence checks and internal/Firm approval of the AR and relevant individuals.

The list of entities which are currently ARs for the Firm at any given time can be checked against the Firm's FCA register entry, and the AR section. This also lists previous ARs under 'previously attached to'.

List of the Firm's ARs

1.5.2 FCA Approved Individuals

There are currently 2 regimes for FCA approval of individuals conducting certain functions within the regulatory perimeter, which staff members need to be aware of:

1. The Senior Managers and Certification Regime (SM&CR): this regime came into force for all solo-regulated, directly authorised firms on 9 December 2019. As such, the Firm is in scope of the SM&CR but this regime does not currently apply to ARs.
2. The Approved Persons regime: this regime continues to apply to ARs.

The regimes, and the functions that are most likely to apply to the Firm and its ARs, are covered in more detail in Chapter 5A and 5B. It is important for all staff members to note that **where a function does apply, advance FCA approval must be obtained before an individual carries out the function(s) in question.**

2 HIGH-LEVEL PRINCIPLES

2.1 Introduction

The FCA operates an **outcomes-focused approach** to regulation, where it measures defined outcomes and acts on the results with relevant firms where results indicate intervention is needed. Outcomes-focused regulation means, amongst other things, looking at what firms must achieve by way of outcomes for the benefit of clients but also the public interest.

This Manual reflects the FCA's approach of focusing on, and taking quick action to achieve, the best outcomes for clients as well as the Firm's approach to compliance with the detailed rules in the FCA's Handbook.

It is the responsibility of all partners, staff members and ARs to be familiar with the FCA Principles for Businesses (see section 1.3). **The Principles are to be adhered to at all times by all partners, staff members and ARs, both in letter and in spirit.** This imposes an additional responsibility beyond the requirement to comply with the procedures set out in this Manual. It will never be adequate to defend conduct that fails to conform to the Principles simply by maintaining that that conduct satisfied the prescribed procedures; compliance with both at all times is mandatory.

It is the Firm's policy that whereas the Principles for Businesses are expressed as obligations on the Firm itself, these are also to be treated as directly applicable to all ARs of the Firm and all individuals within the Firm and an AR. Not all of the Principles will be equally relevant to each individual (e.g. many in the Firm will have nothing to do with the maintenance of the Firm's financial resources – Principle 4), but the Principles are to be interpreted broadly and, where in any doubt, regarded as applicable. Some of the Principles are directly relevant to all (e.g. conducting the Firm's business with integrity) and must be borne in mind at all times. Staff members must report to the Compliance Officer if:

- They know or suspect that they have or anyone else in the Firm or an AR has breached any of the Principles.
- They consider that any of the Firm's procedures is inconsistent with the Principles.
- They are asked, directly or indirectly, to act in a way that they consider breaches any Principle.

Breaches of the Principles can lead to disciplinary action by the FCA against the Firm and damage to the Firm's reputation. Every individual is responsible for taking all reasonable steps to prevent any of these situations arising by strict adherence to the Principles at all times. Failure to do so will be treated as a breach of contract and may lead to dismissal, AR termination and/or withdrawal of FCA approval.

2.2 Treating Customers Fairly

The Firm and its ARs are obliged to treat all customers/clients fairly (Principle 6). It is the responsibility of the Firm's/AR's senior management to ensure that this is being done. Senior management must ensure that a Treating Customers Fairly (TCF) culture is implemented and embedded throughout the Firm and its ARs. The Firm acknowledges that it is the responsibility of everyone in the Firm and within its ARs to deliver TCF.

The Firm has its own policy in regard to TCF. This policy can be found at Appendix G. However, it also expects all ARs to either adopt this policy and/or implement their own similar policy.

2.3 Conduct Risk

The Firm considers conduct risk both for itself and its ARs on an ongoing basis as part of its corporate governance and AR supervision structure and as part of its annual AR monitoring programme. Conduct risk is not defined by the FCA but is described as 'what good looks like'. Conduct risk can also be considered to relate to behaviours and events which could occur and could lead to poor or negative regulatory outcomes for clients.

The Firm's definition of conduct risk can include but is not exclusive to:

- The risk that the Firm does not recognise, manage or mitigate any potential conflict of interest which could occur in relation to the AR hosting model and does not align its primary obligations to the underlying clients or investors of the ARs, rather than the ARs themselves.
- The risk of ARs not understanding their responsibilities under, and the regulatory limitations relating to, the AR–principal arrangement, as detailed in the AR agreement and initial training material.
- The risk that the senior management of the ARs are not fit and proper – see FIT criteria.
- The risk that the Firm's oversight processes, both internal and those for its ARs, are ineffective.

More granular risks that underpin the Firm's definition include: non-competent staff or failure of staff to maintain their competence and capability; lack of documented and effective procedures, systems and controls; and staff acting without appropriate permissions/authorisation or outwith internally agreed authorities. It could also relate to ineffective business models and inappropriate firm culture.

To identify, manage and minimise these risks where possible, and address these issues, there is an appropriate Firm corporate governance framework including:

- Regular (monthly to 6-weekly), documented Firm management meetings, which all internal members attend and which are recorded/minuted.
- A Primary Contact structure so that each AR has an allocated member of the compliance team to act as a central point of contact for defined compliance oversight responsibilities.
- A documented AR onboarding and due diligence process which includes a risk assessed questionnaire to be completed prior to review and a decision being taken to onboard an AR.
- A documented AR monitoring process including at least annual risk-based formal reviews including financial assessment of the AR and F&P checks (i.e. honesty, competence and financial soundness) on AR Approved Persons.
- A structured and risk-assessed monthly AR reporting process, based on quantifiable KPIs on which all ARs are assessed and a consolidated report produced.
- Quarterly feedback to ARs on the above monthly reporting process and KPIs.
- A documented escalation process highlighting steps that may be taken to manage any non-compliance of the ARs with the Firm's overall oversight and contractual arrangements.
- Appropriate due diligence and staff competence assessments prior to approval.
- Documented procedures, including 'know your client' and client categorisation procedures.
- Initial and ongoing compliance training, and regular guidance and information on regulatory trends and developments issued to ARs and staff.
- A transparent complaints process.
- Control over financial promotions and relevant initial and ongoing training.
- Operational controls and clear restrictions over investment management activities.

3 SENIOR MANAGEMENT ARRANGEMENTS, SYSTEMS & CONTROLS (SYSC)

3.1 Introduction

SYSC is the framework for orderly management and conduct of the Firm's business. It also creates a common platform of organisational systems and controls for firms subject to CRD and/or UK MiFID. The Firm is a common platform firm.

In summary, the SYSC rules outline collective and individual accountability of firms' senior management to take practical responsibility for the conduct and actions of their firms and adequate risk management systems which the FCA will expect to see. Ultimately, the partners and senior management of the Firm will be held responsible for the organisation and actions of the Firm and the regulated activities of the Firm's ARs for which the Firm is taking responsibility, as outlined in each AR agreement. AR senior management are also responsible and accountable for all the activities of their own firms. The FCA rules on SYSC are contained in the SYSC sourcebook in line with the following application, SYSC Allocation SYSC 4.1.

3.2 Allocation of Responsibilities and Oversight

Following the FCA principles-based approach to regulations, the Firm has implemented the following policy in line with Principles for Businesses 3 and SYSC 4. SYSC 4.3 refers to those senior personnel who effectively direct the business and make up the Firm's Governing Body.

Under the requirements in SYSC 4.3.1 R, the Firm is required to ensure that senior personnel are responsible for ensuring that the Firm complies with its obligations under the regulatory system. In particular, senior personnel must assess and periodically review the effectiveness of the policies, arrangements and procedures put in place. These must comply with the Firm's obligations under the regulatory system and the Firm should take appropriate measures to address any deficiencies.

Oversight responsibilities are the collective responsibility of senior personnel.

SYSC 4.3.2 R requires a firm to ensure that senior personnel receive, at least annually, written reports on the effectiveness and adequacy of policies and procedures in relation to regulatory compliance and risk control.

The Compliance Officer and Money Laundering Reporting Officer (MLRO) will each prepare a written report to the Governing Body on an annual basis in the respective areas of responsibility.

3.2.1 Policy

To ensure a high level of corporate governance, the Firm will maintain clear and appropriate allocation of significant responsibilities (as well as Prescribed Responsibilities (PRs), as required under SM&CR) amongst partners and senior managers. The Governing Body will appropriately allocate to one or more individuals the responsibility for overseeing the establishment and maintenance of systems and controls under SYSC to one or more individuals.

3.2.2 Allocation and Oversight Procedures

The following procedures and arrangements are in place:

- Clear and appropriate allocation of significant responsibilities amongst partners and senior managers is essential for ensuring there are no gaps in governance and that the business and the affairs of the Firm can be adequately monitored and controlled by the Governing Body. The Compliance Officer will maintain a SYSC Responsibilities Table (see Appendix A2) which documents the allocation of PRs and the main business areas for which each senior manager or partner at the Firm is responsible. This allocation will be reviewed annually or more frequently if the circumstances change.
- The Firm will maintain a record of the arrangements it has made to satisfy the SYSC requirements and take reasonable care to keep this up to date. The relevant records for this purpose will include (but not necessarily be restricted to) Statements of Responsibility, organisational charts, business risk assessments including responsibilities, Governing Body minutes and staff job descriptions. In line with good practice, these records must be maintained for 5 years from the date of origin, and where superseded by a more up-to-date record (e.g. where job responsibilities are materially changed over time), a clear and consistent version-controlled record retention process must be observed. The Compliance Officer will maintain these records.

3.3 Governing Body Meetings

The Firm will hold regular meetings, periodically and as and when required, where partners and, where relevant, senior managers will report on all activities. As referred to in the above section, areas of responsibility will be established, and the appropriate individuals will be obliged to provide updates to the Governing Body at these meetings. The meetings will be appropriately minuted and records kept. At present, due to the size of the Firm, the partners are involved in all decision-making for the Firm and no actions are delegated to any sub-committees.

3.4 General Organisational Requirements

SYSC 4.1.1 requires the Firm to have robust governance arrangements taking into account the nature, scale and complexity of the business. These include a clear organisational structure with well-defined transparent and consistent lines of responsibility. These also include effective processes to identify, manage, monitor and report the risks the Firm is, or might be, exposed to. Finally, the Firm should have internal control mechanisms including sound administrative and accounting procedures, as well as effective controls and safeguarding arrangements for information processing systems.

In order to comply, the Firm will undertake the following:

3.4.1 Decision-Making and Organisational Structure

As to decision-making procedures and a clear and properly documented organisational structure with well-defined, transparent and consistent lines of responsibility:

- The Compliance Officer will maintain organisational charts which clearly specify reporting lines and allocate functions, PRs and other responsibilities. Any changes in these will be provided to the Governing Body for ratification and approval, subject to prior approval from the FCA where applicable, and then communicated to the Firm and its ARs as appropriate.
- Documented Statements of Responsibilities setting out relevant Senior Management Functions (SMFs) and PRs.
- Documented role profiles (including a definition of the role) and all responsibilities and limitations will be authorised by the Governing Body and maintained by the Compliance Officer.

3.4.2 Identifying, Managing, Monitoring and Reporting Risk

As to processes for identifying, managing, monitoring and reporting risk:

- Partners and senior managers are required to furnish the Governing Body at each meeting with the information, in relation to each of their responsibilities, that the Governing Body needs in order to play its part in identifying, measuring, managing and controlling risk.

3.4.3 Internal Control Mechanisms and Administrative Accounting

As to internal control mechanisms and administrative accounting procedures:

- The Firm is required to implement and maintain adequate internal control mechanisms designed to secure compliance with decisions and procedures at all levels of the Firm. The Firm is also required to maintain effective internal reporting and communication at all relevant levels of the Firm.
- SYSC also requires the Firm to ensure that it can monitor and verify its compliance with the relevant prudential supervision requirements under the Investment Firms Prudential Regime (IFPR). The Compliance Officer in conjunction with the other partner(s) will monitor and ensure that the management accounts can verify at all times the Firm's compliance with the capital resource requirement rules detailed in SYSC and MiFIDPRU.
- SYSC 4.1.5 R requires the Firm to have systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information.

3.5 Business Continuity Policy (BCP)

SYSC 4.1.6 to 4.1.8 requires the Firm to establish, implement and maintain an adequate BCP aimed at ensuring, in the case of any interruption to its systems and procedures, that the Firm can continue to conduct its business by limiting losses, preserving essential data and functions or where it is not possible, resume its business in a timely manner by recovering such data and functions, which takes into account:

1. Resource requirements such as people, systems and other assets, and arrangements for obtaining these resources.
2. The recovery priorities for the Firm's operations.
3. Communication arrangements for internal and external concerned parties (including the FCA, ARs, clients and investors, and the press).
4. Escalation and innovation plans that outline the processes for implementing the plan, together with relevant contact information.
5. Processes to validate the integrity of information affected by the disruption.
6. Regular (at least annual) testing of the BCP (and recording thereof) in an appropriate and proportionate manner to evaluate the adequacy and effectiveness of the plan and take appropriate measures to address any deficiencies.

A full detailed BCP plan is maintained separately. The Compliance Officer will update the BCP whenever there is a material change to the Firm's operations, structure, business, location or regulations. In addition, the BCP will be regularly reviewed and if relevant, tested.

3.6 Data Security and Confidentiality

3.6.1 Introduction

SYSC 4.1.5 requires firms to put in place systems and procedures to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question. SYSC 13.7 (although not directly applicable to the Firm) additionally requires firms to maintain systems and controls for the management of IT risks and information security.

The Firm is not required to appoint a data protection officer. However, the Firm has allocated data protection responsibility jointly to the Compliance Officer and MLRO. They are responsible for data security arrangements within the Firm. The Firm has a documented data security procedure in place describing these arrangements that is reviewed on an annual basis as part of an overall annual review of the Firm's systems and controls. The Firm takes a proportionate, risk-based approach to data security taking into account its customer base, business and risk profile. The Firm will also consider any associated risks regarding outsourcing its IT arrangements, including third-party support or platforms including cloud-based computing.

3.6.2 Secure Environment

- All staff are required to keep a clear desk in relation to client-related information.
- All staff are required to lock their PCs/laptops when not in use.
- All staff are required to make use of any confidential waste bins/shredding facilities for the disposal of confidential or sensitive data.
- Access to IT systems containing customer data, both through laptops and desktops, is controlled using individual user accounts that are password protected.
- Anti-spyware software and firewalls are used to protect IT systems.
- All confidential and sensitive data held by the Firm in paper form is stored in lockable filing cabinets.
- All information collected for KYC purposes can only be accessed by staff who require this information to do their jobs.
- Systems prevent unauthorised access to buildings and IT systems when staff leave the Firm.

3.6.3 Staff

- Staff training is tailored to ensure that staff understand the Firm's data security procedures.
- Staff have been made aware that all data security breaches must be reported to the Compliance Officer.
- There is a risk-based approach to staff recruitment, with higher vetting standards for staff with access to confidential or sensitive data where required.
- When staff leave, all their IT access rights are permanently disabled.
- If data is lost, it is the Firm's policy to inform affected customers of the data loss in writing, unless the data is encrypted or where there is law enforcement or regulatory advice to the contrary.

3.6.4 Confidentiality

Confidentiality is of fundamental importance to the maintenance of the Firm's integrity, reputation and professional standing. Staff must not discuss with partners/shareholders, clients, ARs, contacts, family or friends any information they may have about the Firm's or ARs' clients or any business where the Firm is involved.

3.7 Data Protection Act 2018

The Data Protection Act 2018 replaced the previous 1998 Act and enacted the General Data Protection Regulation (European Parliament and Council Regulation 2016/679) on 25 May 2018. It is available to view at this link.

The core principles and their implementation are set out below:

- **Lawfulness, Fairness and Transparency** – the Firm only holds data it is required to hold to comply with FCA requirements and data subjects have the right to request their data at any time.
- **Purpose Limitation** – the Firm only holds data it is required to hold to comply with FCA requirements and does not use this data for any other purpose.
- **Data Minimisation** – the Firm only holds data it is required to hold to comply with FCA and legal requirements.
- **Accuracy** – the data subject has the right to request a copy of their data at any time and to rectify it if required.
- **Storage Limitation** – the Firm will only hold on to the data for the period it is legally required.
- **Integrity and Confidentiality** – the Firm is committed to keeping its customers' data safe by storing it on reputable cloud-based platforms and in locked cupboards only. Data may be shared where legally required.
- **Accountability** – the Firm commits to its accountability for maintaining the core principles as set out above.

The Firm and each AR should understand whether, under the Data Protection Act 2018 and UK GDPR, they are a controller, joint controller or processor in respect of AR client business. To help with this understanding, the creation of a data flow chart is recommended, analysing the data held, why it is held, what is done with it and to whom it may be disclosed, transferred, etc.

Some firms have the mandatory requirement to appoint a data protection officer (DPO). This does not apply to the Firm. However, responsibility for data protection has been jointly assigned to the Compliance Officer and the MLRO.

Under the Data Protection Act 2018, fines can extend to a maximum of 4% of annual worldwide turnover or €20m for some breaches.

3.7.1 Response Procedure for Data Subject Rights Requests

Firms must have in place response procedures for requests to:

1. Access personal data.
2. Rectify personal data.
3. Erase personal data.
4. Restrict the processing of personal data.
5. Port personal data (where applicable).
6. Object to the processing of personal data.

Where there are joint controllers, the data subject must be notified of this at the earliest opportunity.

It should be noted that some data subject rights are not absolute and only apply in certain circumstances.

3.7.1.1 Subject Access Requests

Individuals have the right to access their personal data and can make a subject access request verbally or in writing. Firms should have a policy in place to deal with such requests. Firms must respond within one month (from the day the request is received) and cannot charge a fee for the majority of requests.

More information on access requests is available on the ICO website.

3.7.1.2 Rectify Personal Data

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. The request can be made verbally or in writing, and firms must respond to the request within one month.

More information on rectifying personal data is available on the ICO website.

3.7.1.3 Erasure of Personal Data

Individuals have the right to have their personal data erased, known as 'the right to be forgotten'. This only applies in certain circumstances, such as when the personal data is no longer necessary for the purpose for which it was originally gathered.

More information on erasure of personal data is available on the ICO website.

3.7.1.4 Restricting the Processing of Personal Data

Individuals have the right to request the restriction of their personal data. This only applies in certain circumstances. Firms must respond within one month (from the day the request is received).

More information on the restriction of personal data is available on the ICO website.

3.7.1.5 The Portability of Personal Data (where applicable)

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The right only applies to information an individual has provided to a controller.

More information on the restriction of personal data is available on the ICO website.

3.7.1.6 Objections to Processing of Personal Data

Individuals have the right to object to processing of their personal data in certain circumstances. An individual can make an objection verbally or in writing. Firms have one calendar month to respond to the objection.

More information on the right to object is available on the ICO website.

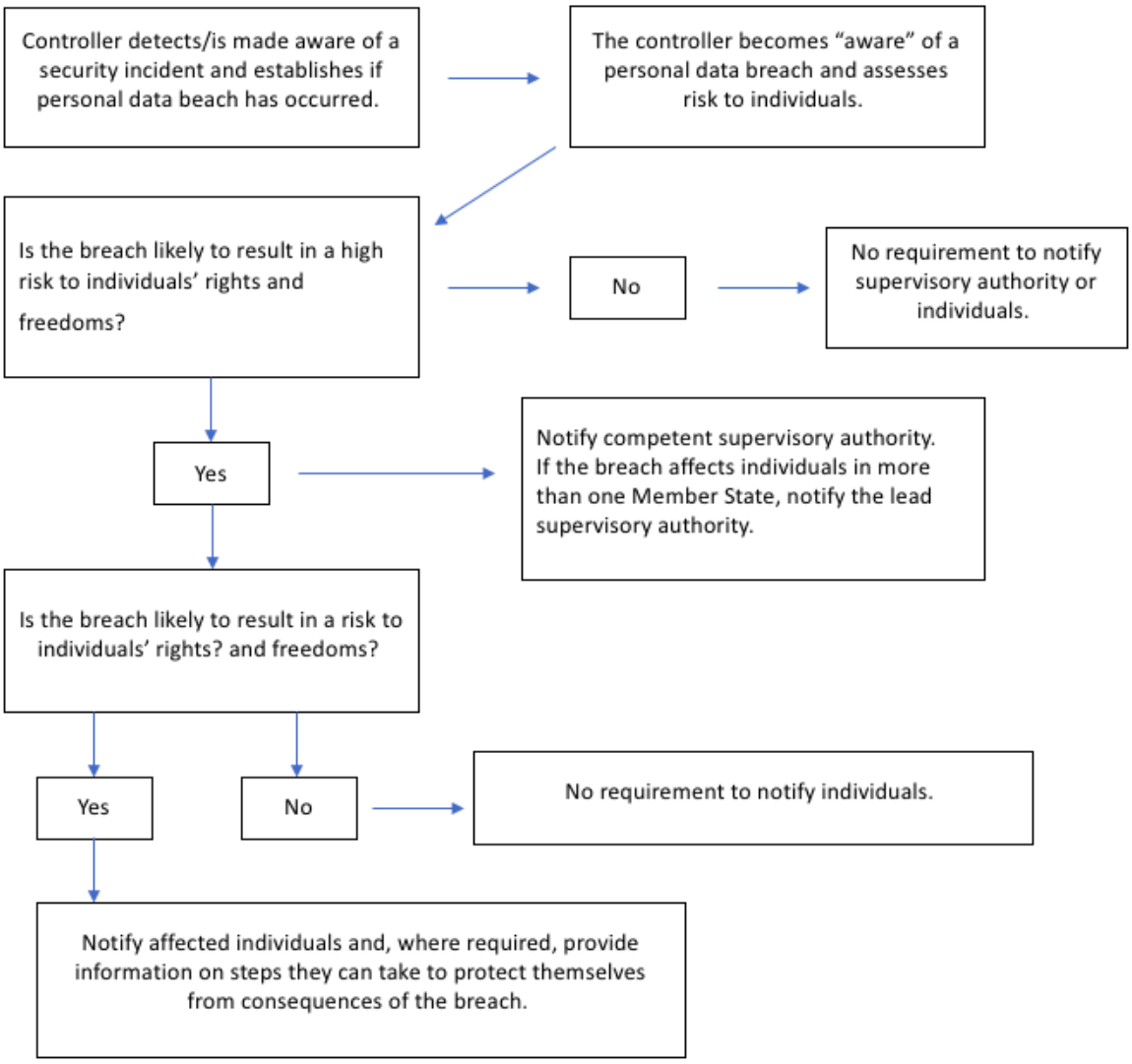
3.7.2 Personal Data Breach Notification

A personal data breach notification is defined by the ICO as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

Examples of breaches include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

In case of a breach, firms are required to follow the following chart in order to determine whether a notification should be made:



If applicable, firms are required to notify affected data subject(s) within 24 hours of becoming aware of the breach and the supervisory authority, the ICO, within 72 hours. The notification must be done by either the DPO, Compliance Officer, or another person who is responsible for data protection. All breaches, even those of a not notifiable nature, must be documented and the record maintained by the controller.

Where there is a joint controller, the party which becomes aware of a breach, needs to confirm with the other party that a breach has indeed occurred and agree and document who will be responsible for notifications.

3.7.3 Data Protection Impact Assessments (DPIAs)

3.7.3.1 Introduction

Article 35(1) of the GDPR requires the Firm to conduct a DPIA before it begins any type of processing that is likely to result in high risk to individuals' interests. In other words, where there is the potential for widespread or serious impact on individuals.

A DPIA is a procedure to systematically analyse processing and help identify and minimise data protection risks. The process does not have to eradicate the risk but should help to minimise risks and help the Firm consider whether or not the residual risks are justified.

The DPIA must include:

- A description of the processing and purposes.

- An assessment of necessity and proportionality.
- An assessment of risks to individuals.
- Details of measures to mitigate those identified risks and protect the data.

If the DPIA identifies high risks that cannot be mitigated the Firm's Compliance Officer must consult the ICO.

In addition to complying with the specific provisions of the GDPR, DPIAs help the Firm demonstrate accountability and can bring also bring about broader compliance, financial and reputational benefits. DPIAs can help the Firm develop relationships of trust with its customers and help demonstrate compliance with FCA Principles 1, 2 and 3.

3.7.3.2 Circumstances Requiring a DPIA

The Firm must do a DPIA if it plans to:

- Use systematic and extensive profiling with significant effects.
- Process special category or criminal offence data on a large scale.
- Systematically monitor publicly accessible places on a large scale.

The ICO also requires the Firm to do a DPIA if it plans to:

- Use new technologies.
- Use profiling or special category data to decide on access to services.
- Profile individuals on a large scale.
- Process biometric data.
- Process genetic data.
- Match data or combine datasets from different sources.
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing').
- Track individuals' location or behaviour.
- Profile children or target services at them.
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

In addition to the above situations, the Firm will consider doing a DPIA for any other processing which is large scale, involves profiling or monitoring, involves decisions on access to services or opportunities, or involves sensitive data or vulnerable individuals.

The Firm will also do a DPIA for any major new projects involving the use of personal data even if there is no specific indication of likely high risk, as it is considered good practice.

A single assessment to address a set of similar processing operations that present similar high risks is permitted.

DPIAs will also be added as an agenda item to the Firm's management meeting when relevant to identify where DPIAs are needed and to provide updates to management on DPIAs currently in progress.

3.7.3.3 Procedure for Conducting a DPIA

DPIAs should be conducted, where appropriate (see above), before the Firm starts processing. In practice, DPIAs should run alongside the planning and development phase and include the following steps:

- Identify the need for a DPIA: what are the objectives of the processing and what is involved.
- Processing description: nature, scope, and purposes.

- Consultation: identify relevant stakeholders and experts, describe when and how their views/advice will be sought.
- Assessment of:
    - Necessity and proportionality: identify lawful basis, alternative ways of achieving the same/similar outcomes, how adherence to GDPR provisions/principles will be ensured.
    - Risks and mitigating measures: source, likelihood, severity and overall score of risks, along with mitigating actions, their likely effect on risk and the residual risk.
- Sign-off and record-keeping: review, comments and feedback by Compliance Officer and then management team before implementation.
- Integration: with existing processes and procedures, e.g. compliance monitoring, and training material.
- Monitoring and review: ongoing oversight and periodic assessment.

Before completing a DPIA, staff should review DPIA guidance from both the ICO and the Article 29 Working Party. The ICO's DPIA template should then be completed and sent to the Firm's Compliance Officer for review, comment and approval before being sent to the wider team for discussion and minuted ratification.

3.8 Accounting Policy

SYSC 4.1.9 R requires a firm to establish, implement and maintain accounting procedures and policies that enable it to deliver in a timely manner to the FCA financial reports of its financial position in compliance with current accounting standards and rules.

The Firm has engaged Chiene and Tait, a firm of accountants based in Edinburgh and experienced in audits for FCA-regulated firms, to carry out a formal audit of its account at least annually. The Firm uses Xero, an online software accounts package, to prepare its own management accounts to assist the Firm to monitor its financial position to verify compliance with the FCA's Capital Resources Requirements. The preparation of the management accounts will also enable the Firm to deliver in a timely manner the financial reports required by the FCA.

3.9 Regular Monitoring

SYSC 4.1.10 R requires the Firm to monitor and, on a regular basis, evaluate the adequacy and effectiveness of its systems and controls and take measures to address any deficiencies. This is carried out on an ongoing basis by the Compliance Officer with support from the compliance team, especially where the Compliance Officer may have been involved in the activities being monitored and to ensure independence. Regular monitoring and oversight is also conducted on its ARs.

As already discussed, the Firm has regular Governing Body meetings where partners and senior managers will report to the partners. From time to time, the Firm may also engage with an independent provider of compliance monitoring services to supplement internal monitoring.

3.10 Audit Committee

An Audit Committee has not been formed due to the size of the Firm's business activities, low numbers of staff and simple business operations. Arrangements to ensure the effectiveness of systems and controls are as described elsewhere in this Manual.

3.11 Persons Who Effectively Direct the Business

SYSC 4.2.2 R requires the Firm to ensure that its management is undertaken by at least 2 senior personnel of sufficiently good repute and experience so that they can ensure sound and prudent management of the Firm. This ensures that at least 2 independent judgements have been applied in the formulation and implementation of the policies of the Firm.

The senior personnel include partners or persons granted executive powers by, and reporting directly into, the Governing Body who are involved in directing the business.

3.12 Skills, Knowledge and Expertise

SYSC 5.1.1 requires the Firm to employ personnel with skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.

The Firm is required to have systems and controls to enable the Firm to satisfy itself of the suitability of anyone who acts for it.

An individual's honesty and competence assessment will be made at the point of recruitment taking into account the level of responsibility the individual will assume in the Firm. All new members of internal staff will undergo a full interview, vetting and reference verification process. Those requiring FCA approval will, at either the Firm or AR level, go through appropriate due diligence in accordance with relevant FCA rules.

When the Firm intends to recruit new staff members not personally known by a senior member of the Firm, at least 2 employment references must be sought and verified (where feasible) and recruitment procedures will mirror FCA rules even if the individual is not to become FCA approved. Where the individual is personally known by a senior member, a discretionary decision that at least one employment reference must be sought and verified. However, normally 2 will be requested and covering at least 6 years of employment where relevant.

More details on the requirements of the Firm with respect to competence of individuals are in the Training and Competence section of this Manual.

Where the individual is to be undertaking a Controlled Function (ARs only) or Senior Management Function (the Firm only), they must be registered with the FCA as an Approved Person before engaging in the relevant activity.

3.12.1 Segregation of Functions

SYSC 5.1.6 R requires the Firm to ensure that the performance of multiple functions by its relevant persons does not, and is not likely to, prevent those persons from discharging any particular functions soundly, honestly and professionally.

SYSC 5.1.7 R requires the Firm to define arrangements concerning segregation of duties within the Firm and the prevention of conflicts of interest.

The purpose of these rules is to ensure that no single individual is completely free to commit the Firm's assets or incur liabilities on its behalf. Segregation also helps to:

1. Ensure that the partners receive accurate and objective information on financial performance, the risks faced by the Firm and the adequacy of its systems.
2. Ensure staff members do their jobs honestly and professionally.
3. Prevent/manage conflicts.
4. Ensure no unrestricted authority combining front, middle and back office.

5. Ensure compensating controls where full segregation is not possible.

No single individual will have unrestricted authority to do all of the following primarily concerning client-related investment transactions:

1. Initiate a transaction.
2. Bind the Firm.
3. Make payments.
4. Account for the transactions.

The Compliance Officer will monitor and on a regular basis evaluate the adequacy of the segregation of duties at the Firm as a measure of an effective internal control, taking into consideration any conflicts of interest. Nominated senior managers at ARs should do the same.

3.12.2 Awareness of Procedures

SYSC 5.1.12 R requires that the Firm must ensure that all relevant staff members are aware of the procedures which must be followed for the proper discharge of their responsibilities. All staff have access to this Manual, as this is held online, and will also have been provided with any separate operational procedures that exist. These procedures are reviewed at least annually.

3.13 Compliance, Internal Audit and Financial Crime

SYSC 6.1.2 requires the Firm to establish and maintain policies and procedures designed to detect and minimise risk of failure by the Firm to comply with its obligations under the regulatory systems and enable the FCA to exercise its powers effectively.

The purpose of SYSC 6.1 is to ensure that the Firm has in place and maintains adequate policies and procedures sufficient to ensure compliance of the Firm. This includes its managers, staff members and anyone who works on behalf of the Firm or under its scope of permission (i.e. its ARs) with the obligations under the regulatory system and for countering the risk that the Firm might be used to further financial crime.

SYSC 6.1.3 R requires the Firm to have and maintain a compliance function which operates independently of the Firm's regulated activities and discharges its responsibilities properly. This includes monitoring and assessing the effectiveness of the compliance procedures. This also includes taking action to address any deficiencies in the Firm's compliance procedures in addition to advising and assisting the Firm to comply with its obligations under the regulatory system.

Given the size of the Firm and the scale of its business, the Firm has considered that it is not yet appropriate or necessary to have a fully separate, permanent compliance function. The Compliance Officer function is held by one of the partners whose responsibilities include monitoring and assessing the effectiveness of the compliance procedures and taking action to address any deficiencies in the Firm's compliance procedures. This is in addition to advising and assisting the Firm to comply with its obligations under the regulatory system.

Through Gillian Gallacher as Compliance Officer, the Firm also engages with Gem Compliance Consulting Ltd, which is a member of the Association of Professional Compliance Consultants, and an independent compliance consultancy, to provide compliance resources and support on its behalf which includes:

- Monitoring, including written reports where appropriate.
- Formal annual monitoring of the Firm's ARs.
- Documentation of internal compliance procedures and training materials.

- Identifying and addressing compliance training needs.
- Maintaining a compliance diary and appropriate registers/records.
- Assisting in the completion of regulatory returns.
- Ensuring that the Manual and monitoring plans remain up to date.
- Advising on any forthcoming regulatory developments which may impact on the Firm.

SYSC 6.1.4 R requires the senior management to ensure the Compliance Officer has the necessary authority, resources, expertise and access to all relevant information to carry out the role.

The Compliance Officer is responsible for preparing a written report directly to the senior management on an annual basis or more frequently depending on changes in regulation or business. The report should cover the adequacy and effectiveness of the compliance measures and procedures put in place to minimise the risk of failure of the Firm, including those who are employed by the Firm, to comply with its regulatory requirements.

The Compliance Officer's responsibilities include:

1. Providing advice on the regulatory implications of new regulations and changes to the business profile.
2. Arranging for periodic compliance monitoring on the basis of a risk-based compliance monitoring programme.
3. Making and effecting recommendations for improvements regarding the manner in which compliance is achieved.
4. Preparing written annual reports on compliance matters for the Governing Body.
5. Ensuring that regulatory compliance risk is taken into account in the Firm's day-to-day operations.

3.13.1 General Policy

The Compliance Officer should not be involved in the performance of services or activities that they are responsible for monitoring and all remuneration policies are set by the Governing Body. The Compliance Officer is not a Certified staff member and is therefore independent of client-related regulated activities.

However, due to the size of the business activities, numbers of staff members and simple business operations, the Firm's Compliance Officer may be involved in associated operational issues. If this occurs, the Governing Body of the Firm will ensure that there will be no link between the Compliance Officer's remuneration or incentives and the operational issues they become involved in.

3.13.2 Internal Audit

SYSC 6.2.1 R requires the Firm to establish and maintain an internal audit function which is separate and independent from the other functions and activities of the Firm.

In essence, the purpose of SYSC 6.2 is to maintain an audit plan to assess the adherence to and effectiveness of the internal systems and controls, procedures and policies, and to provide a written annual report of its findings and recommendations to the Governing Body.

An internal audit function has not been formed due to the size of the business activities and straightforward operational structure. Arrangements to ensure the effectiveness of systems and controls are as described elsewhere in this Manual.

3.14 Risk Control and Management

The purpose of SYSC 7.1 is to set out the policies for the management of risks ('risk policy') faced by the Firm. It is intended that the policies meet the requirements of the Governing Body, to run the business in accordance with regulatory requirements.

SYSC 7.1.2 R requires the Firm to have in place effective processes to identify and assess the risks relating to the Firm's activities, processes and systems it is, or might be, exposed to and to have in place mechanisms to control and manage these risks. The Firm identifies and assesses its risks primarily through a quarterly review of the Firm's Risk Register which is reflected in the Internal Capital and Risk Adequacy Assessment (ICARA). It may also use other risk management tools and records where necessary. It is the responsibility of the Compliance Officer to maintain appropriate risk management arrangements along with any other partners. At the AR level, it is the responsibility of each nominated senior manager to ensure its ARs maintain appropriate risk management arrangements. This includes maintenance of a similar Risk Register and process.

According to SYSC 7.1.4 R, the Governing Body must approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks the Firm is or might be exposed to including those posed by the macroeconomic environment in relation to the business cycle, taking into account:

1. The adequacy and effectiveness of the risk management policies and procedures.
2. The level of compliance by the Firm and its relevant staff members with the arrangement put in place to manage risks.
3. Adequacy and effectiveness of measures taken to address any deficiencies in risk management policies and procedures, including failure by relevant staff members to follow such policies and procedures.

3.14.1 Sources of Risk

Risk can arise from the investment and advisory process, the Firm's ARs, the Firm's business systems and operational procedures, both internal and/or external sources including economic and political changes, and staff. Losses to any clients can have an effect on the reputation of the Firm and in some cases could require compensation by the Firm. Therefore, risks to clients that can be linked to the Firm's actions are regarded as priority risks.

The Compliance Officer will be responsible for ensuring that the controls put in place to mitigate specific risk are monitored, and for suggesting areas for improvement as appropriate to the Governing Body, who will then be involved in any implementation and follow-up. The ICARA assessment (as described in Chapter 6 of this Manual) will be reviewed at least on an annual basis or more frequently if there are major changes to the business, regulations and/or external situations beyond the Firm's control.

3.14.2 Credit and Counterparty Risk

Through the use of appropriate and effective systems, the Firm must operate the ongoing administration and monitoring of any credit risk-bearing exposures (those of the Firm, not of its clients).

In the Firm's case, its credit/counterparty risk is the risk that its ARs (debtors) do not pay their invoices. As such the Firm is required under the rules to determine if there is a need for an increase in its capital resource requirement on an ongoing basis. Fees are invoiced monthly and in advance and therefore the position is monitored regularly and at least monthly. Capital required to satisfy capital adequacy is appropriately ring fenced separately from working capital as part of the Firm's risk management process.

3.14.3 Market Risk

The Firm will not have traditional trading book market risk as it does not trade the Firm's capital on a proprietary basis. The Firm does play any action role in the investment transaction 'chain' (where one exists) between its ARs and the ARs' underlying clients. The Firm is subject to non-trading book market risk, i.e. the market risk of assets held on its balance sheet and the performance risk of any funds that it is responsible for.

The only potential key exposures are non-trading book exposures to foreign currency assets or liabilities held on the Firm's balance sheet. At present, the Firm does not hold significant currency assets or liabilities on its balance sheet, and the majority of assets are held in cash. Therefore, currency exposure risk is considered low unless this position changes.

3.14.4 Interest Rate Risk

Interest rate risk is not applicable to the Firm and as such no procedures are currently required to manage that risk.

3.14.5 Business and Operational Risk

The Firm implements policies and processes to evaluate and manage the exposure to business and operational risk, including low-frequency, high-severity events.

Business risk is defined as any risk to the Firm arising from changes in its business, including the risk that the Firm may not be able to carry out its business plan and its desired strategy.

As part of FCA supervision, the Firm is required to meet threshold conditions at all times. This includes conditions regarding its business model which will be assessed by the FCA at authorisation as to whether it is acceptable and also to identify any underlying risks. As part of the ICARA process, or on an ad hoc basis, the Firm will review its business model to ensure that it continues to satisfy this threshold condition.

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

The risk category includes real risks to the Firm, such as outsourcing risk associated with key service providers, such as:

- Bookkeeping and IT.
- Key individuals leaving and internal disputes.
- Provision of poor services.
- Bad publicity.
- Politics/terrorism.
- Loss of key clients and/or investors.
- Regulatory breaches and risks including market abuse.
- Money laundering etc.

These risks are assessed in the ICARA and the Firm's Risk Register.

3.15 General Outsourcing Requirements

SYSC 8.1 states that the Firm must take reasonable steps to avoid undue additional operational risk when relying on a third party for the performance of operational functions which are critical for the performance of regulated/ancillary activities.

Although the Firm is not in scope of the Operational Resilience arrangements under SYSC 15A, introduced by PS21/3 in March 2022, it may also consider this chapter as guidance where this might relate to outsourcing an 'important business service' (as defined).

In accordance with Principle 11, if the service provider performs a process, service or activity the Firm would otherwise do itself and this activity is an investment service or critical to the regulated activities, the Compliance Officer must notify the FCA that it is relying on a third party for critical operational functions (see SUP 15.3.8(e)).

Where relevant services are outsourced, the Firm and its senior management remain fully responsible for discharging all of its obligations under the regulatory system. This also applies to ARs.

Relevant outsourcing should not:

1. Create additional operational risk.
2. Jeopardise internal controls.
3. Delegate responsibility or change client relationships.
4. Hinder the FCA/internal compliance monitoring.
5. Prevent continued compliance with the threshold conditions.

SYSC 8.1.5 gives guidance on certain functions not normally considered to be material outsourced functions, e.g. legal advice, personal training, billing, security, and standardised services such as market information services and price feeds as these are not considered critical for the performance of regulated business.

The Firm (and ARs) must use due skill, care and diligence when entering into and managing or terminating any arrangements for the outsourcing to a service provider of critical operational functions. In essence the Firm/ARs must make sure the service provider is competent (and is an Authorised Person if necessary), have a written agreement which clearly allocates and sets out rights and responsibilities, and which ensures effective performance against agreed standards, e.g. service level agreement, regular review and monitoring, escalations, service credits etc.

In summary, the service provider is required to:

1. Have their own appropriate supervision, policy and procedures.
2. Have their own risk management arrangements.
3. Disclose material developments.
4. Co-operate with the FCA.
5. Give the Firm, auditors and FCA effective access to data and premises.
6. Protect confidential information.
7. Have an appropriate BCP and regular back-up testing.

In summary, the Firm/its ARs are required to:

1. Retain expertise to supervise and manage effectively.
2. Take action if problems appear.
3. Have power to terminate the outsourcing agreement without detriment to client service.
4. Have a BCP and regular back-up testing.

The Firm does not outsource any of its investment management or advisory activities. Any advisory activities that are provided by its ARs are operated as separate businesses and not on the Firm's behalf. As such there is no outsourced operational risk to be taken into account within this sphere of regulated activities. It has certain functional support, and the above principles are applied where appropriate as best practice.

The Governing Body will keep under review all potential outsourced services that do not currently form part of the regulated activities of the Firm, to ensure these remain non-material outsourced functions.

Under the Data Protection Act 2018 and UK GDPR, the Firm is also responsible to ensure that its data processors comply with relevant rules under the Data Protection Act and it is recommended that these checks are evidenced. Where processors are located outside the UK, the Firm/AR should ensure they are registered under a regime considered equivalent, e.g. the EU's GDPR, or use an appropriate and formally recognised mechanism, e.g. standard contractual clauses.

3.16 Remuneration

SYSC 19 covers systems and controls on remuneration ('the Remuneration Code'). Specifically SYSC 19G covers MiFIDPRU investment firms and with MiFIDPRU 8.6 covering remuneration disclosure requirements. The FCA consider that firms need to align remuneration policies with effective risk management. SYSC 19 is split into sections with each section applying to specified categories of firms. The Code at SYSC 19G (relevant to IFPR firms) contains a number of Principles that all firms must comply with as a minimum. There are additional Principles or requirements that certain firms must additionally comply with depending upon the nature of their business and organisation. The Firm is required to comply with the minimum Principles due to proportionality.

SYSC 19F also applies to the Firm in relation to remuneration incentives and performance management of all staff. The Firm does not operate a specific incentive system for staff based on performance of either its staff or a particular investment or AR.

Material Risk Takers (as defined) includes all partners of the Firm but also any other Approved Persons and persons who may be involved in exercising judgement on significant risks on behalf of the Firm.

The Firm has a separate remuneration policy documented to satisfy SYSC 19G which takes into account the following:

- Confirmation that the Firm is within scope of SYSC 19G.
- Identifying who Material Risk Takers are.
- Summarising the Firm's existing remuneration structure.
- Outlining which Principles the Firm is required to comply with.
- Outlining how the Firm complies with these Principles or explaining any other arrangements, including what if any balance there is between variable and fixed remuneration.
- Arranging for annual disclosure on its website, in line with MiFIDPRU 8.6, at the same time that its annual financial statements are published at Companies House.

3.17 General Rules on Record-Keeping

SYSC 9.1 requires the Firm to retain all records kept by it under SYSC for a period of at least 5 years after last use in a readily available but appropriately secure medium, so that records can be easily accessed as and when required.

As noted above, the Firm will keep all records for at least 5 years but this may be longer subject to data protection legislation and guidance. ARs should also incorporate these retention periods into their own record-keeping policies. All staff are responsible for ensuring that records in their relevant areas are not deleted or destroyed. Any questions or requests to delete records must be made to the Compliance Officer.

3.18 Conflicts of Interest

SYSC 10.1.3R requires the Firm to take all appropriate steps to identify and prevent, or where conflicts cannot be prevented, effectively manage or mitigate any conflicts of interest:

1. Between the Firm (including its managers, staff members or any person directly or indirectly linked to them by control) and a client of the Firm
2. Between one client of the Firm and another client

that arise or may arise in the course of providing any services in relation to the Firm's regulated investment business activities. ARs should also adhere to these requirements and the requirement explained immediately below.

SYSC 10.1.7 R requires the Firm to maintain and operate effective organisational and administrative arrangements to prevent conflicts of interest from arising, or if they do arise, from damaging or giving rise to a risk of damage to the interests of its clients.

Under SYSC 10.1.10 R the Firm has established a conflict of interests policy (see Appendix D) which:

1. Identifies the circumstances (although the list is not exhaustive) which constitute or may give rise to a conflict of interest entailing a material risk of damage to the interests of one or more clients.
2. Specifies procedures to be followed and measures to be adopted in order to manage such conflicts.

As a mechanism for identifying, preventing, managing, monitoring and mitigating conflicts of interest the Compliance Officer maintains a conflicts of interest register on behalf of the Firm in which a conflict of interest entailing a risk of damage to the interests of clients has arisen (or may arise) and identifying mitigating controls and responsibilities. Where appropriate, conflicts at AR level are also recorded by the Firm.

3.19 Obligations for Telephone and Electronic Communications

SYSC 10A.1.6R requires the Firm (and relevant ARs) to 'take all reasonable steps to record telephone conversations and keep a copy of electronic communications [not limited to emails], that relate to the activities in financial instruments referred to in SYSC 10A.1.1R(2) (and that are not excluded by SYSC 10A.1.4R), and that are made with, sent from, or received on, equipment' either provided by firms or permitted for use by firms. As such, firms must prevent the use by staff of devices where firms are unable to record or copy relevant communications.

The telephone calls and electronic communications that should be recorded are those that are intended to result in the performance of relevant activities in relation to specified financial instruments (see above rule references) even if the communications do not actually result in the performance of such activities.

Face-to-face conversations can be recorded using written minutes or notes but must include at least the following:

- Date and time of meetings.
- Location of meetings.
- Identify of attendees.
- Initiator of meetings.
- Relevant information about the order.

Relevant records must be stored in a durable medium that allows them to be replayed and copied. They must be provided to clients upon request, subject to Data Protection Act provisions, and kept for at least 5 years or, where requested to do so by the FCA, up to 7 years, from the date of creation.

Where call recording is required, the Firm and its ARs are required to notify clients about call recording before services are provided. The Firm and ARs are also required to inform clients about the retention requirements applying to such conversations.

Additional requirements are contained in Article 76 of the MiFID Org Regulation and include the establishing, implementing and maintaining of an effective policy (see Appendix R) covering the recording of relevant telephone conversations and electronic communications. The policy should cover:

- How relevant conversations and communications are identified and the procedures to be followed.
- Periodic evaluation of the policy and associated procedures.
- Periodic monitoring of relevant calls.
- Management body oversight and control of relevant policies and procedures.
- Individuals and devices covered by the policy.

3.20 Outside Business Interests

3.20.1 Introduction

The Firm's staff and partners are required to obtain prior approval from the Compliance Officer, or another partner if the Compliance Officer is making the request, before acquiring an interest in any outside business organisation, and in particular before becoming a partner, director, officer or adviser of a company whether or not it is a paid position. Requests for such approval should be sent in writing (email) to the Compliance Officer who maintains a record. AR staff should also notify the Firm before becoming a partner, director, officer or adviser in an outside organisation, regardless of whether or not it is a paid position.

The approval for the Firm's staff regarding outside business interests will not be unreasonably withheld, but it must be clearly understood that any outside employment or business interests must not be carried out on the Firm's premises nor shall it conflict or interfere with the Firm's business in any way.

The Firm's staff must notify the Compliance Officer of the following:

- Any current or past directorships or partnerships during the previous 10 years.
- Any organisation in which a member of staff owns more than 1% whether or not they are a director/partner of that organisation.
- Consultancies paid or unpaid (now or in the last 10 years).
- Trusteeships paid or unpaid (now or in the last 10 years).
- Any other relevant interests, e.g. part-time work etc.

Staff will be requested to provide information on any such potential conflicts of interest arising from outside interests either when joining the Firm as an internal person or before an application is submitted to the FCA for the performance of a specified function. Please note that staff, FCA approved individuals (under both regimes) and Certification staff are obliged, on an ongoing basis, to notify the Compliance Officer of all new outside business interests, of any changes to the information already disclosed or of any additional information regarding interests previously disclosed that has subsequently come to light.

3.20.2 Suppliers

Staff are required to disclose to the Compliance Officer any monetary connections which they or any member of their family have with any person or firm which supplies goods or services to the Firm or which has done so in the last 6 months, to the Compliance Officer. Usual business courtesies can be disregarded.

3.20.3 Interests in Competitors

Staff may not participate as an employee, director, partner, consultant or shareholder or in any other way in any outside business whose services or products compete, directly or indirectly, with those offered by the Firm. This prohibition does not apply to ownership of less than 1% of the issued shares of a publicly traded company.

3.20.4 Publicly Traded Companies

No member of staff may accept a directorship of a publicly traded company unless approval has been obtained in advance from the Compliance Officer who may in turn may seek approval from other senior management if appropriate. This also applies to AR staff. Directorships of publicly traded companies that are held by any members of their immediate family should be notified to the Compliance Officer.

3.21 Whistleblowing

The Governing Body is committed to maintaining the highest standards of honesty, openness and accountability and recognises that all partners and other members of staff have an important role to play in achieving this goal.

Staff may often be the first to suspect, identify and/or know when someone inside or connected with an organisation may be doing something improper, but may feel apprehensive about voicing their concerns. This may be because they feel that speaking up would be disloyal to their colleagues or the organisation itself. It may also be because they do not think that their concerns will be taken seriously or because they are afraid that they will be penalised in some way. However, the Firm does not believe that it is in anyone's interest for staff with knowledge of wrongdoing to remain silent.

The Firm takes all malpractice very seriously, whether it is committed by senior managers, staff, suppliers, ARs or contractors; this document sets out a procedure by which staff can report their concerns. ARs are encouraged to establish their own, equivalent policies or they can formally adopt the approach detailed below.

3.21.1 The Public Interest Disclosure Act 1998

The Public Interest Disclosure Act 1998 amended the Employment Rights Act 1996 to give protection from victimisation and dismissal to individuals who make certain disclosures in the public interest.

In normal circumstances a ‘qualifying disclosure’ is one which satisfies the 3 criteria below:

1. It is made in good faith.
2. It is made in the reasonable belief that the information disclosed tends to reveal one or more of the following:
    - That a criminal offence has been, is being or is likely to be committed, e.g. tax evasion, or the facilitation of tax evasion.
    - That there has been, is, or is likely to be, a failure to comply with a legal obligation, e.g. failure of the Firm to prevent tax evasion.
    - That the health or safety of any individual has been, is being, or is likely to be endangered.

- That the environment has been, is being, or is likely to be damaged.
- That information that shows one of the above has been, is being, or is likely to be concealed.

3. It is made to one of the following:
   - The employer (or the person specified by the employer under any internal whistleblowing procedure).
   - Where the disclosure concerns the actions of a person other than the employer, that person.
   - If the disclosure is made in the course of obtaining legal advice, a legal adviser (the requirement for 'good faith' does not apply here).
   - In the case of employers of non-departmental public bodies, the relevant government minister.
   - Where the worker additionally believes that the allegation and any information contained in the allegation is substantially true, a person or body prescribed by the Secretary of State.

Aside from the Public Interest Disclosure Act 1998, all staff remain obligated to follow compliance reporting as outlined in this document and any other Firm policy documents.

3.21.2 Reportable Activities

It is impossible to give an exhaustive list of the activities that constitute malpractice but, broadly speaking, the Firm would expect its staff to report the following:

- Criminal offences.
- Failure to comply with legal obligations or applicable regulations.
- Miscarriages of justice.
- Actions which endanger the health or safety of staff or the public.
- Actions which cause damage to the environment.
- Actions which are intended to conceal any of the above.

It will not always be clear that a particular action falls within one of these categories, and partners and other members of staff must use their own judgement in this regard. However, the Firm would prefer staff to report their concerns rather than keep them to themselves. If a report is made in good faith, even if it is not confirmed by an investigation, the initial concern will be valued and appreciated, and staff will not be liable to disciplinary action. If a false report is made, maliciously or for personal gain, then disciplinary action may result.

Please note that this procedure is not a substitute for the Firm's (or an AR's) grievance procedure which should be used if members of staff have a complaint or concern in relation to any internal procedure or action which affects their employment or working arrangement directly.

3.21.3 Making a Report

A report can be made verbally or in writing. The Firm would normally expect concerns to be raised internally to a designated partner.

Which of these individuals is the more appropriate will depend on the seriousness of the alleged malpractice and who the reporting member of staff thinks is involved. If they have not already done so, the partner may request that the reporting member of staff clearly sets down their concerns in writing, together with any evidence supporting the concerns.

Please note that regardless of the above, any suspicion of money laundering or related financial crime must be reported to the Firm's **MLRO, or in the absence of the MLRO, the Deputy MLRO**. This should also be done where there may be a suspicion of market abuse.

The Firm does not expect the individual making the report to have absolute proof of any alleged malpractice. However, they will need to be able to show the reason for their concern.

The Firm will do everything possible to keep the identity of the reporting individual secret, if they so wish. However, there may be circumstances where their identity needs to be disclosed (e.g. if the report becomes the subject of a criminal investigation wherein they may be needed as a witness) or where their identity may need to be disclosed to the regulatory authorities. Should this be the case the matter will be discussed with the individual at the earliest opportunity.

3.21.4 Investigating Reports

Once a report has been made, the Firm will acknowledge receipt of it within 5 working days. The Firm will endeavour to deal with any concerns raised under this procedure quickly and efficiently.

There are, of course, 2 sides to every story and the Firm will need to make preliminary enquiries to decide whether a full investigation is necessary. If such an investigation is necessary then, depending on the nature of the misconduct, the initial concerns will be either:

- Investigated internally (by senior management).
- Referred to the appropriate external person (e.g. external auditors, the FCA or the police) for investigation.

Subject to any legal constraints, the Firm will inform the reporting member of staff of the outcome of the preliminary enquiries, full investigation and any further action that has been taken.

If the reporting members of staff are unhappy with the outcome of an investigation, the Firm would prefer that another report was submitted explaining why this is the case. The fresh concerns will subsequently be investigated if there is good reason to do so.

However, it may be that the reporting individual does not think that this process is appropriate and wishes to raise their concerns with an external organisation, such as a regulator. It is, of course, open for them to do so provided that they have sufficient evidence to support their claim.

Financial Conduct Authority

- FCA's direct whistleblowing number is 020 7066 9200
- FCA's direct email address is whistle@fca.org.uk
- For further information see https://www.fca.org.uk/firms/whistleblowing

Please send letters to:

Intelligence Department (ref PIDA)
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

The Firm strongly advises that before staff report concerns externally, independent advice is sought from the following:

Protect (formerly Public Concern at Work)

Tel: 020 3117 2520
https://protect-advice.org.uk

Whilst the Firm cannot guarantee that it will respond to the report in the way that the reporting individual might wish, it will try to handle the matter fairly and properly. This will be achieved by using the above procedure.

4 FINANCIAL CRIME

4.1 Introduction

SYSC 6.1.1 R requires the Firm to implement and maintain adequate policies and procedures for countering the risk that the Firm might be used to further financial crime.

As an authorised principal to a number of ARs, the Firm is also responsible for supervising its ARs' compliance with relevant financial crime requirements by monitoring and enforcing compliance with the financial crime policies and procedures contained within the Manual.

Financial crime is defined under FSMA to include any offence involving:

- Fraud or dishonesty.
- Misconduct in, or misuse of information relating to, a financial market.
- Handling the proceeds of crime.
- The financing of terrorism.

The FCA's Financial Crime Guide contains practical assistance and information for firms of all sizes and across all FCA supervised sectors on actions they can take to counter the risk that they might be used to further financial crime, generally and in relation to specific risks, such as fraud and money laundering.

4.1.1 Awareness of and Training of Staff

Appropriate training will be provided to all members of Firm staff, Approved Persons and relevant AR employees/staff members as notified by the AR to the Firm, in relation to anti-money laundering in accordance with SYSC 6.3.7 G. The training forms part of the induction process for new joiners and part of the onboarding process for ARs and is repeated at least once every 12 months for all Approved Persons and relevant staff of the Firm. The MLRO is responsible for updating, or arranging the updating of, the financial crime training and it is the MLRO who should be contacted with any questions in this regard. However, annual review of financial crime training forms part of the annual review of all online training modules, which is arranged by the Compliance Officer. The compliance team, under the supervision of the Compliance Officer, keeps a record of the date the training was given, the nature of training, names of staff who received the training and results of tests undertaken by staff, where appropriate.

4.1.2 MLRO and Other Arrangements

SYSC 6.3.8 R requires that the Firm allocate to a partner or senior manager (who can also be the MLRO) overall responsibility within the Firm for establishing and maintaining effective money laundering systems and controls. This responsibility (and the corresponding Prescribed Responsibility (d) under the SM&CR) has been allocated to Kevin Gallacher.

SYSC 6.3.9 R requires the Firm to appoint an individual as the Firm's MLRO with responsibility for oversight of the Firm's compliance with the FCA's rules on systems and controls against money laundering. Senior management must ensure the MLRO has sufficient seniority and has access to resources and information to carry out the role. The FCA expects the Firm's MLRO will be based in the UK and must be an FCA Approved Person.

Under Regulation 21(3) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (as amended) (the MLRs 2017), the Firm is required to name a Nominated Officer to receive and review internal disclosures (suspicious activity reports or SARs) under Part 7 of the Proceeds and Crime Act 2000 (POCA) and the Terrorism Act 2000 (TA).

Emma Jones is the Firm's MLRO and Nominated Officer with both roles being collectively referred to as the MLRO role in this Manual. She has been approved by the FCA to undertake SMF 17 – MLRO function, and acts as the focal point for the oversight of all activity relating to anti-money laundering. She can pass on issues to the National Crime Agency (NCA) and request a defence to a money laundering offence, as appropriate. The MLRO is able to monitor day-to-day operations of anti-money laundering policies within the Firm and is able to respond promptly to any reasonable request for information made by the NCA, FCA or another enforcement body.

Queries from ARs relating to the Firm's financial crime policies and procedures should be directed to their Primary Contacts in the first instance. Submission of suspicious activity reports (SARs) should be sent *directly and confidentially* to the MLRO/Deputy MLRO, as outlined in the relevant section below.

In the MLROs absence queries should be directed to the Deputy MLRO, Gillian Gallacher. If the position of MLRO falls vacant, a replacement will be appointed by the management Governing Body and registered as an Approved Person for SMF 17 with the FCA.

The **MLRO's responsibilities** include:

1. Receiving internal reports of suspected money laundering from within the Firm.
2. Reporting to NCA.
3. Obtaining and using national and international findings.
4. Overseeing adequate arrangements within the Firm for money laundering awareness and training in line with current legal and regulatory requirements.
5. Maintaining anti-money laundering record-keeping arrangements.
6. Making annual reports to senior management about money laundering compliance in respect of criminal property, money laundering and terrorist financing risks.
7. Ensuring that money laundering risk is taken into account in the Firm's day-to-day operations, e.g. development of new products, taking on of new customers and changes in business profile.
8. Ensuring appropriate documentation of risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies.

4.1.3 Record-Keeping

Copies of client identification evidence must be retained for a minimum of 5 years from the end of the relationship with the client. Transaction records must be retained for 5 years from the end of the business relationship or after the date of an occasional transaction. Notwithstanding this, it is the intention of the Firm to retain ALL records for a minimum of 5 years. Training records should include when anti-money laundering training was given.

Upon the expiry of the 5-year period the Firm must delete any personal data unless either:

- The Firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings.
- The data subject has given express consent to the retention of that data.

Although a regulatory or legislative requirement can override a data subject's rights, information need not be kept beyond 10 years for any transaction during a business relationship even if the business relationship has not ended.

4.2 Market Conduct

Both insider dealing and market manipulation meet the FSMA definition of financial crime. In December 2018, the FCA updated its Financial Crime Guide (FCG) and the FCG now includes a chapter on insider dealing and market manipulation – FCG 8.

4.2.1 Insider Dealing

Insider dealing is made a criminal offence in Part V, section 52 of the Criminal Justice Act 1993 (CJA). The CJA makes it an offence to use non-public price-sensitive information (inside information) in order to make a profit or avoid a loss when dealing in securities, derivatives or other investments ('securities') or to enable anyone else to do so. It is also possible for a transaction which involves insider dealing to constitute a breach of the Law and incur penalties otherwise than under the insider dealing provisions of the CJA.

Importantly, under insider dealing legislation, potential liability can continue for at least as long as the information is not made public, so staff members' responsibilities may not cease upon leaving the Firm.

4.2.2 Market Manipulation

Under sections 89-91 of the Financial Services Act 2012, certain behaviours (collectively referred to as 'market manipulation') amount to criminal offences:

- Misleading statements – making false or misleading statements, promises or forecasts, dishonestly conceals or withhold any material facts.
- Misleading impressions – any action or course of conduct that creates a false or misleading impression of the market. This could include giving advice recklessly.
- Misleading statements or impressions in relation to benchmarks.

The penalty on conviction of a criminal offence of insider dealing or market manipulation can be up to 10 years' imprisonment and an unlimited fine. Furthermore, under common law a client may sue the Firm for damages. It should be noted that most legal actions under these sections of FSMA are likely to be taken against staff members of firms rather than firms themselves.

4.3 Market Abuse

The EU's Market Abuse Regulation (EU MAR) came into effect on 3 July 2016 and was onshored through the Market Abuse (Amendment) (EU Exit) Regulations to create the UK's Market Abuse Regulation (UK MAR). Changes were made to EU MAR to reflect the UK's new position outside the EU and to ensure UK MAR operates effectively in the UK. Changes were also made to ensure the UK's overseas territories are within the scope of EU MAR. However, the policy approach of EU MAR was not altered through onshoring. Therefore, in practical terms firms should not experience significant changes under UK MAR.

UK MAR contains the following legislation, technical standards and guidance:

- EU Market Abuse Regulation as amended by the Market Abuse Exit Regulations 2019 (therefore, the 2 sets of regulations need to be read together).
- FCA Technical Standards relating to UK MAR.
- ESMA Guidelines and ESMA questions and answers that existed before the end of the transition period.
- FCA guidance: FCA Handbook.

UK MAR aims to increase market integrity and investor protection, enhancing the attractiveness of securities markets for capital raising. It contains prohibitions of insider dealing, unlawful disclosure of inside information and market manipulation, and provisions to prevent and detect these.

The FCA's webpage on the Market Abuse Regulation aims to assist readers of the FCA's Handbook and contains links to relevant information sources.

MAR 1 of the FCA's Handbook MAR sourcebook provides assistance in determining whether or not behaviour amounts to market abuse. However, it should be noted that the chapter does not exhaustively describe all types of behaviours that may indicate market abuse.

Six types of behaviour (market conduct) are defined as market abuse by the Market Abuse Regulation:

1. Insider dealing (Handbook reference: MAR 1.3).
2. Unlawful disclosure (Handbook reference: MAR 1.4).
3. Manipulating, or attempting to manipulate, transactions (Handbook reference: MAR 1.6).
4. Manipulating devices (Handbook reference: MAR 1.7).
5. Dissemination (of false or misleading information) (Handbook reference: MAR 1.8).
6. Misleading behaviour and market distortion (Handbook reference: MAR 1.9).

The above headings are elaborated on below. Full descriptions/explanations and links to relevant articles of the regulation are available in the MAR sourcebook of the FCA's Handbook. The scope of investments covered by the regime is also detailed and this can include, in some cases, indices not just qualifying securities.

It is an offence to carry out any activity that amounts to market abuse.

4.3.1 Insider Dealing

Insider dealing is dealing, or attempting to deal, on the basis of inside information. Inside information is defined under Article 7 of UK MAR as information that:

- Is precise in nature.
- Has not been made public.
- Relates, directly or indirectly, to one or more issuers or financial instruments.
- If made public, would likely have a significant effect on the prices of those, or related derivative, financial instruments.

Information would be considered 'precise' if it indicates a set of circumstances which exists or may reasonably be expected to come into existence, or an event which occurred or may reasonably be expected to occur, specific enough to conclude as to its possible effect on the prices of the financial instruments or related derivative financial instrument (Article 7.2).

UK MAR also clarifies that using inside information to amend or cancel an order shall be considered insider dealing.

Examples of insider dealing include front running/pre-positioning; dealing or attempting to deal whilst in possession of inside information concerning a proposed takeover bid.

4.3.2 Unlawful Disclosure

Unlawful Disclosure refers to disclosing information relating to qualifying investments other than in the proper course of professional duties.

UK MAR has clarified that recommending or inducing another person to transact on the basis of inside information also amounts to unlawful disclosure of inside information.

Examples include: selective briefing of analysts; selective/unprofessional disclosure of information by the directors of an issuer.

4.3.3 Manipulating, or Attempting to Manipulate, Transactions

Manipulating, or attempting to manipulate, transactions refers to trading activity that could create a misleading impression as to the supply of, demand for, or price of qualifying investments.

Examples include: buying or selling at the close of the market with the effect of misleading investors who act on the basis of closing prices; sale or purchase where there is no change in beneficial ownership effected with the intention of misleading investors; entering orders into an electronic trading system and withdrawing them before they are executed with the intention of misleading investors; abusive squeezes.

4.3.4 Manipulating Devices

Manipulating devices refers to employing fictitious devices or any other form of deception with regard to a qualifying investment.

Examples include: voicing an opinion about a qualifying investment whilst holding a position in the investment and profiting subsequently from the effect of the market acting on that opinion; a series of transactions that are designed to conceal the ownership of a qualifying investment so that disclosure requirements are circumvented by the holding of the qualifying investment in the name of a colluding party, such that disclosures are misleading in respect of the true underlying holding.

4.3.5 Dissemination (of False or Misleading Information)

Dissemination (of false or misleading information) is the distribution of information which gives a false or misleading impression as to a qualifying investment. Dissemination of misleading information or unsubstantiated rumour is regarded as market abuse (see the Firm's policy at Appendix I).

4.3.6 Misleading Behaviour and Market Distortion

Misleading behaviour and market distortion refer to actions (e.g. physical movement of commodity stocks) that could create a misleading impression as to the supply of, demand for, or price of a qualifying investment.

4.3.7 Examples of Market Abuse

Please refer to Appendix H for specific examples of what may or may not constitute market abuse.

4.3.8 Suspicious Transaction and Order Reports (STORs)

Under UK MAR, firms that professionally arrange or execute transactions in certain financial instruments (as specified in Article 4 of UK MAR), and operators of UK trading venues, must report suspicious transactions and orders (STORs), or suspicions of attempted market abuse, to the FCA without delay through the Connect system using the STOR form. For further information on reporting suspected market abuse to the FCA, visit the FCA's dedicated webpage.

A suspicious transaction or order is one where there are 'reasonable grounds' to suspect it might constitute market abuse, such as insider dealing or market manipulation.

Staff members should decide on a case-by-case basis whether there are reasonable grounds for suspicion, taking into account the deciding circumstances, e.g. elements constituting market abuse, any other behaviour or information. Note that it may not always be apparent that a transaction might be abusive

until after a transaction has taken place. However, firms should not breach information barriers to prevent and avoid conflicts of interest in order to detect suspicious transactions/orders.

The FCA has incorporated the STOR requirements of UK MAR into SUP 15.10 of its Supervision Manual and in SUP 15 Ann 5, the FCA has provided some indicators of possible suspicious transactions or orders.

STORs should only be used to report potential market abuse under Article 16 of UK MAR, not other types of suspicion or incidents.

Currently, the Firm and its ARs do not arrange or execute any relevant transactions. If an AR were to do this and a suspicious transaction/order was encountered, a STOR should be made by email to the Firm's MLRO or Deputy MLRO who will make the report to the FCA on behalf of the AR. When initially making the internal STOR, please include the following details and attach relevant supporting documentation:

- Transaction/order number.
- Description of the nature of the suspicion.
- Identity/identifying details of entity/person suspected.
- Additional information.

For more information on suspicious transaction and order reporting, market abuse risks, transaction reporting, and other market conduct issues, refer to the FCA's Market Watch newsletters.

The UK applies an 'all crimes' approach to money laundering meaning that insider dealing and market manipulation are predicate offences to money laundering. Therefore, the Firm, ARs and associated individuals need to also consider their obligations under POCA and TA including the submission of a SAR as well as a STOR to the MLRO and tipping off.

4.3.9 Manager's Transactions

UK MAR Article 19 requires persons discharging managerial responsibilities within certain issuers (PDMRs), and persons closely associated with them (PCAs), to notify the FCA and the issuer of relevant personal transactions they undertake in the issuer's shares, debt instruments, derivatives, or other linked financial instruments, if the total amount of transactions per calendar year has reached €5,000. The issuer in turn must make that information public within 2 working days of receipt of the notification from the PDMR.

This requirement applies to:

- Issuers who have requested or approved admission of their financial instruments to trading on a UK regulated market.
- In the case of instruments only traded on a UK MTF or on a UK OTF, issuers who have approved trading of their financial instruments on a UK MTF or a UK OTF or have requested admission to trading of their financial instruments on a UK MTF.
- UK EAMPs (emission allowance market participants) in relation to transactions in UK emission allowances and related auction products and derivatives.

Given the business model of the Firm and its ARs and the instruments in which they deal, it is considered that notifications under Article 19 of UK MAR do not apply to the Firm or its ARs.

4.3.10 Significant Short Positions

The EU Short Selling Regulation (EU SSR) and Level 2 Regulation were converted into UK law along with Binding Technical Standards at the end of the transition period forming the UK's Short Selling Regulation (UK SSR).

The UK SSR applies to the short selling of sovereign debt, shares that are admitted to trading on a UK trading venue, and related instruments, and the use of credit default swaps (although an exemption for shares exists where the principal trading venue of a share is located in a third country).

It requires holders of net short positions in shares admitted to trading on a trading venue in the UK (unless they are exempt) or UK sovereign debt to make notifications to the FCA once certain thresholds have been breached. Further information on notification and disclosure of net short positions is available from the FCA. The UK SSR also outlines more restrictions on investors entering into uncovered short positions in shares or UK sovereign debt.

The UK SSR provides for certain exemptions for market-making activities and primary market operations. However, the FCA points out that the exemptions cannot be automatically used, are limited and only apply to specific instruments. For further information, see the FCA's note on the UK notification process for market makers and authorised primary dealers under the UK SSR.

The FINMAR section of the FCA Handbook applies to all natural and legal persons to whom the short selling regulation applies.

Under FINMAR 2.5, the FCA may take measures to prohibit, restrict, manage or limit transactions in short positions. This will depend upon a number of different factors as detailed in FINMAR 2.5. Where this is imposed the Firm and its ARs will comply with any current requirements where relevant. However, given the business models of the Firm and its ARs, the SSR is unlikely to apply and where it does the Firm is unlikely to have any significant short positions in the majority of situations.

4.3.11 Risk Assessment

Given the nature of the Firm's business, the Firm views its market conduct risk to be low. However, the Firm recognises that staff may receive inside information in the following situations:

- During the fund close process when the Firm is acting as AIFM or sub-manager and reviewing information provided by prospective investors.
- When reviewing investment advice/recommendations as part of monitoring/oversight but also when acting as AIFM/sub-manager.
- When answering ad hoc queries from ARs or enquiries from prospects/other clients.
- When reviewing independent/non-independent research papers prior to issue.

The Firm considers that, in addition to the above scenarios, ARs may also receive inside information when:

- Researching investments.
- Providing investment advice to, or arranging investments for, listed or soon to be listed companies, either directly or indirectly.
- Conducting due diligence on potential portfolio targets or new mandates/clients/investors.
- A portfolio company becomes listed or becomes the target of a listed entity.

ARs should consider their market conduct risks as part of their firm-wide risk assessments and should put in place processes that complement (but not replace) the Firm's policy and procedures below. This risk assessment should be reviewed quarterly.

4.3.12 Policy and Procedure

The FCA expects senior management to take responsibility for its firm's measures in relation to insider dealing and market manipulation. This includes:

- Understanding the risks of insider dealing/market manipulation that their firm is exposed to (through staff member and client activity).

- Establishing adequate policies and procedures to counter these risks in accordance with SYSC 6.1.1R.

Each staff member and Approved Person shall be given access to a copy of this Manual, which contains a summary of the UK's Insider Dealing Regulations and Market Conduct Rules in the FCA's Handbook upon joining the Firm. It is the responsibility of ARs, and the nominated senior managers specifically, to decide who within their firms should be provided with access to the Manual, required to sign the compliance undertaking, and undergo relevant training as part of induction and annually thereafter.

No individual (director, partner, employee or member of staff) should agree to become an insider in relation to the securities of any company other than where this is *necessary* to perform their role as an investment professional of the Firm. **If an individual feels it necessary to become an insider in order to properly perform their professional role, *advance* notification of this intention should be made using the procedure outlined below. The Firm's Compliance Officer will enable the individual to be compliantly 'wall crossed' (see below) and the security to be added to the insider or restricted lists**. All instructions from the Compliance Officer must be followed completely, correctly, and promptly. The individual should also follow any wall-crossing obligations of the company/party involved.

No member of staff should behave in a way that amounts to market abuse. If in doubt, then guidance should be sought from the Compliance Officer.

Staff members should be aware that they may be made an insider in meetings/conversations and if it is the case that they do not wish to be restricted from dealing in the relevant shares, they should make the other party aware that they do not want to be given inside information.

Staff members should also be aware that information provided to an individual may become inside information by virtue of other information they already hold.

In the event that they do come into possession of inside information and pre-clearance was not possible, they must report this as per the procedure below. The Compliance Officer will add the security to the insider or restricted lists. They must also follow the directions of other compliance/legal departments connected to the transaction for which they have been made an insider.

No individual may personally deal in any security about which the Firm has inside information and is listed on the insider list or restricted list. In advance of any personal dealing, individuals should check the restricted list and follow instructions in Appendix F1.

No individual may reveal any inside information held by the Firm/an AR to any third party unless it is proper and necessary to do so, and they have advance consent from the Firm's Compliance Officer.

The CJA's provisions and FCA Market Conduct Rules are very complex and, if anyone is in any doubt whether a particular transaction would be prohibited, they should consult the Compliance Officer.

It should be noted that any contravention of the insider dealing legislation may result in summary dismissal without notice or compensation and immediate withdrawal of FCA Approved Person status, where applicable. The FCA and the Firm may discipline staff members that are in breach of UK MAR and the FCA's Market Conduct Rules.

4.3.13 Insider List Procedure

Wall-crossing is the practice of bringing individuals over an information barrier, or 'wall', to confidentially share non-public information about a public security offering before the information is announced to the public.

If/when AR staff come to possess any inside information, ARs must inform either their Primary Contact, who will inform the Compliance Officer, or the Compliance Officer, in advance where possible. Firm staff must inform the Firm's Compliance Officer, without delay, including where advance consent has been sought by the external party.

Upon notification from an AR, the Compliance Officer or Primary Contact under the direction of the Compliance Officer, will send a wall-crossing notice to the wall-crossed individuals at the AR and update the restricted list. The Firm's Compliance Officer will update the Firm's own insider list. Once the inside information has become public (or 'stale'), the AR should notify the Compliance Officer or Primary Contact who will confirm this, update the Firm's restricted list, and then send a 'cleansing notice' to the wall-crossed individuals to confirm they are no longer insiders in respect of a particular security and instruct them to update their own insider list. The Firm's Compliance Officer will, as before, update the Firm's insider list.

Information on who is an insider within the Firm and within ARs (insider list) **must** be kept confidential.

The Compliance Officer is responsible for maintaining the insider list and ensuring that Firm staff have access to inside information on a need-to-know basis. Therefore, completion of the confidential insider list can only be delegated to the Deputy Compliance Officer in the Compliance Officer's absence. Whereas restricted lists and other associated admin may be delegated by the Compliance Officer to a compliance team member, such as the Primary Contact.

The Compliance Officer is also responsible for monitoring Firm staff's personal account dealing.

The nominated senior managers at each AR are responsible for monitoring personal account dealing within their ARs and raising any questions or concerns with their Primary Contact or the Firm's Compliance Officer.

The Compliance Officer, other partners, Compliance Manager and compliance associates are super-insiders, i.e. always insiders due to their involvement in each transaction. However, where applicable, i.e. where inside information is received outside of, or separately to, an individual's role for the Firm, the Firm's staff will notify the Firm's Compliance Officer, and the wall-crossing and subsequent cleansing notices, and the updating of both the restricted and insider lists, at the appropriate time, will be issued/updated by the Firm's Compliance Officer.

4.4 Fraud

Fraud is the act of obtaining by deception money or assets belonging to another which will benefit the fraudster and expose the victim to a loss. Fraud may be committed against individuals and firms, e.g. through:

- The use of false or stolen identities to defraud financial services organisations.
- The use of the internet, e.g. setting up websites purporting to belong to a reputable institution.
- The use of phishing emails, texts or phones calls purporting to be from a known connection or offering something.

The FCA requires firms to take reasonable care to establish and maintain effective systems and controls for countering the risk that they might be used to further financial crime.

For the following reasons, the Firm assesses its fraud risk to be low-moderate:

- Its core business is a non-retail regulatory incubation model and the provision of investment management services.

- Its direct client base is comprised of corporate entities that are led by FCA-approved industry professionals.
- Most communications and activities take place online/using the internet, through emails, Teams and Zoom, which increased during the pandemic and has remained at a higher level than before the pandemic.
- The Firm's Managing Partner will, where circumstances permit, meet potential clients face-to-face before proposing them as a new client and before onboarding. In all other cases, meetings will be conducted remotely via video call.
- The Firm thoroughly vets its ARs and ARs' senior management prior to them being appointed.
- Fund ARs are typically required to appoint a recognised and appropriately authorised administrator and manager for each fund.
- Fund ARs are required to instruct a specialist fund lawyer to assist them with all legal aspects of the fund.
- The Firm does not hold or control client money or other assets.
- The Firm does not operate any sales-driven/volume-based incentive schemes.
- When acting as fund manager, the Firm requires:
    - Investors to sign a Professional Client notice confirming they qualify as a Professional Client and are happy to be categorised as such.
    - Investors to be subject to appropriate KYC/AML checks by fund administrators and for the Firm to have final approval for each proposed investor before acceptance into the fund.
    - Fund advisers to conduct extensive due diligence on proposed investments including on the target company's policies and AML/KYC checks on founders.
    - Investment recommendations to include detailed information about the proposed investment including identifying information about the target company and the industry/market in which the target company operates and its founders/key personnel.
    - Fund advisers to properly monitor use of funds by portfolio companies.
- Funds managed by the Firm normally include one or more large, institutional investors in the first close.
- Higher risk relationships at AR and Principal levels need to be approved in advance by the Firm's senior management.

4.4.1 Fraud Indicators

The following situations may require enhanced due diligence and or/reporting:

- Remote (non-face-to-face) clients.
- Failure/unwillingness to provide name and address ID.
- Lack of photographic name ID.
- Third-party client referrals.
- Unusual/unreasonable client behaviour/transactions.
- Investments advertising exceptionally high returns.
- Investments with celebrity endorsements.
- Investments concerning luxury items.
- Investments in high-risk jurisdictions.
- High net worth private clients.
- Unsubstantiated claims of company performance.
- Use of, or requests to change account details to, accounts with ambiguous names or unconnected third parties for receipt of funds or distributions.
- Requests from investors to transfer interests shortly after closing.

- Unexpected communications instructing action or requesting assistance or offering a benefit. These communications can be from unknown sources or known contacts or purporting to be from known sources, e.g. hacked accounts.

4.4.2 Preventing Fraud

There are numerous ways the Firm protects itself against fraud, which include:

- Established and clear reporting lines.
- Regular analysis and discussion of risks.
- Appropriate and documented internal procedures covering all areas of the business.
- Identifying the source of payments from bank details, electronically (using Xero) and manually.
- Thoroughly investigating requests from investors to change/update information or transfer rights.
- Segregation of duties.
- Thorough and risk-based initial and periodic screening of staff members and agents/ representatives and checks, where relevant, to ensure ARs and individuals meet the FCA's fit and proper test criteria initially and on an ongoing basis.
- Sign-off of new clients, and their associated individuals, at partner level prior to FCA submission.
- Sign-off of high-risk relationships at senior manager level.
- Anti-bribery and corruption guidance.
- Staff training and testing, including on phishing communications and other scams.
- Compliance monitoring programme.
- Detailed and risk-based KYC procedures.
- Robust IT security measures.
- Data protection procedures.
- Circulation of FCA enforcement cases, including those relating to fraud, internally and to its ARs in the form of its monthly newsletter.

More information on counter-fraud measures/activities is available from the following organisations:

- The National Fraud Authority.
- The National Fraud Authority's cross-sector strategy, Fighting Fraud Together, which is endorsed by the FCA.
- Action Fraud, the UK's national fraud and cybercrime reporting centre.
- The City of London Police, which has 'lead authority' status in the UK for the investigation of economic crime, including fraud.
- The Fraud Advisory Panel, which acts as an independent voice and supporter of the counter-fraud community.

If staff members are targeted by fraudsters at work, they should report the incident to the Compliance Officer or MLRO who will report the issue to Action Fraud or the Police. A report may also need to be made report to the Firm's insurer.

If an AR is targeted by fraudsters, , it should report this to the Compliance Officer or MLRO. The AR should then make a report to Action Fraud or the Police. As above, the AR may need to inform their insurer. The AR should keep the Compliance Officer or MLRO updated on developments.

4.5 Data Security

4.5.1 Background

The Data Protection Act 2018 sets out the framework for data protection law in the UK and the UK General Data Protection Regulation (UK GDPR) sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

The UK GDPR and Data Protection Act 2018 (Part 2, General Processing Regime) require the Firm/ARs to implement and maintain adequate policies and procedures regarding data security. The ICO provides guidance on data protection requirements and the responsibilities imposed on data controllers and data processors.

Chapter 5 of the FCA's Financial Crime Guide contains practical assistance and information for firms of all sizes and across all FCA supervised sectors on actions they can take to counter the risk that they might be used to further financial crime in relation to data security.

4.5.2 Risks

Customers and employees regularly provide firms with important personal/sensitive data. If this data is obtained by criminals, they can attempt to use it to their advantage (and the customer's detriment) such as by undertaking transactions in a customer's/employee's name. The Firm and its ARs should be alert to the financial crime risks associated with holding personal or sensitive data and must take special care of it.

4.5.3 Key Principles and Policy

Every business is different and the Firm and its ARs should, therefore, ensure that they have their own specific data security policy appropriately tailored to their business activities and the data they hold. The policy should cover the core principles of the Data Protection Act which are:

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality.
7. Accountability.

In addition, please see below for some self-assessment questions that the Firm/ARs should consider when reviewing its policies and procedures:

- How is responsibility for data security apportioned?
- Has the business ever lost personal/sensitive data? If so, what remedial actions did it take? Did it contact customers? Did it review its systems?
- How does the business monitor that suppliers of outsourced services treat personal/sensitive data appropriately?
- Are data security standards set in outsourcing agreements, with suppliers' performance subject to monitoring?

4.5.4 Systems and Controls

The Firm and its ARs should ensure they put in place systems and controls to minimise the risk that their operation and information assets might be exploited by thieves and fraudsters. Internal procedures such as

IT controls and physical security measures should be designed to protect against unauthorised access to personal/sensitive data. The ICO has published a practical guide to IT security for small firms, but in simple terms security measures should ensure:

- Only authorised people can access personal data.
- Those people can only act within the scope of their authority.
- Where data loss occurs targeted action can be taken quickly to prevent/minimise damage and distress to the individuals concerned.

The ICO has also published a set of 10 quick steps to help businesses improve basic personal/sensitive data security:

1. Take care when printing and copying.
2. Double-check letters/emails before sending.
3. Include a return address on envelopes.
4. Disable auto-fill in your email settings.
5. Close your messaging when screen-sharing or presenting online.
6. Lock your screen when you are away from your desk.
7. Do not let staff share passwords.
8. Send electronic documents securely (e.g. using encryption or password-protection).
9. Send passwords to protected documents separately.
10. Keep your IT systems up to date.

4.5.5 Best Practices

Below are some best practices that the Firm/ARs should ensure their staff are aware of:

- Lock screen.
- Clear desk/office.
- Over-looking.
- Passwords – most secure formats and frequency of change.
- Personal devices – might be within scope of subject access request.
- Data outputs and transfers.
- Removable media – encryption and other conditions of use.
- Remote working – storage and destruction of paper files or documents/notes and electronic devices, do not leave unattended or in plain sight either in a vehicle or in a remote-working location (including at home, in a hotel room or on public transport).

4.5.6 Data Controllers & Data Processors

All ARs are considered by the Firm to be joint data controllers or data controllers in common. If a breach is discovered, the AR/Firm must notify the other and the ICO (where appropriate) within 72 hours. Data processors are required to notify data controllers of all breaches without undue delay.

4.5.7 Penalties

The maximum penalty for a data breach is up to 4% of annual turnover or €20m (whichever is larger).

4.6 Anti-Money Laundering, Counter-Terrorist Financing and Counter Proliferation Financing

4.6.1 Introduction

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. When successful, money laundering enables criminals to maintain control over their proceeds, and ultimately may provide a legitimate cover for their source of income.

The offence of terrorist financing is made up of 2 parts: money generated by acts of terrorism and money intended for use in acts of terrorism.

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of chemical, biological, radiological or nuclear (CBRN) weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

The importance of efforts to tackle these activities is related to the FCA's operational objectives as referred to in Chapter 1 including 'Protecting and enhancing the integrity of the UK financial system'.

The current primary legislations in the UK concerned with anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CTF/CPF) are POCA (as amended including by Serious Organised Crime and Police Act 2005), TA (as amended), which outline the money laundering and terrorist financing offences, and the Sanctions and Anti-Money Laundering Act (SAMLA). In addition, the MLRs 2017 impose obligations on those performing regulated activities.

4.6.1.1 POCA

Under POCA there are 5 basic criminal offences with the penalty for non-compliance ranging from 5 years to 14 years' imprisonment, a fine, or both.

1. **Concealing or transferring criminal proceeds**. Attempts to convert or disguise the proceeds of crime into something appearing legitimate, or transferring money to avoid detection or confiscation, are criminal offences.
2. **Assisting others to launder money**. It is a criminal offence to help others to launder money. 'Assisting' can be any kind of assistance, active or passive.
3. **Acquiring, possessing or using criminal proceeds**. If it is known that money is directly or indirectly the proceeds of a crime, it is an offence to receive, possess or use that money. 'Money' has a wide definition, including property.
4. **Failing to report actual or suspicious money laundering activity**. The duty is on the individual to prove that there were no grounds for suspicion. It is also a criminal offence not to report promptly where there are reasonable grounds for suspicion.
5. '**Tipping off**'. It is a criminal offence to alert a suspected money launderer or accomplice of the fact that an investigation is underway, or report has been made into suspected money laundering.

It is important to note that the POCA offences involve the proceeds of any criminal behaviour, by anyone, anytime, anywhere. This means that funds generated by activities in breach of FSMA would be in scope of POCA. There is, however, one exception to the 'all crimes' application, which is where it is known or there are reasonable grounds to believe that the conduct occurred outside the UK in a jurisdiction in which it was legal under recognised local law.

4.6.1.2 Terrorism Act

Part III of the TA contains offences, including money laundering offences (s18), and imposes an obligation on firms to make reports where they know or suspect, or have reasonable grounds to suspect, engagement in terrorist financing:

- Offences for fund-raising (s15), using and possessing (s16), and arrangements concerned with funding terrorism or controlling terrorist property (s17).
- Specific offence for insurers regarding insurance payments made in response to terrorist demands (s17A).
- Failing to disclose knowledge or suspicion of terrorist financing (s21A).

4.6.1.3 Sanctions and Anti-Money Laundering Act

The SAMLA enabled the UK to create its own sanctions framework and money laundering and terrorist financing regulations autonomously post-Brexit. Numerous sanctions regimes aimed at countering proliferation financing are implemented by this Act.

4.6.1.4 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017)

The MLRs 2017 contain 3 separate criminal offences:

- Contravening a relevant requirement (regulation 86).
- Prejudicing an investigation (regulation 87).
- Providing false or misleading information (regulation 88).

The MLRs 2017 also place a legal requirement on firms to follow a **risk-based approach**, both in respect of risk management generally, and specifically in respect of KYC/AML due diligence measures. The Firm and its ARs are required to take appropriate steps to identify and assess money laundering, terrorist financing and proliferation financing risks, to document risk assessments and keep them up to date. A third party such as an auditor or regulator should be able to understand the decisions made by the Firm/AR from its records.

In assessing financial crime risk, the MLRs 2017 require the Firm to take account of:

- The risks from:
    - Customers and underlying beneficial owners.
    - Products/services.
    - Transactions.
    - Delivery channels.
    - Geographical areas of operation.
- Information made available to them by the FCA, including enforcement findings and consequential actions.
- Risk factors, including factors relating to its customers, countries or geographic areas in which they operate, products, services, transactions and delivery channels.
- Relevant findings in the UK National Risk Assessment of Money Laundering and Terrorist Financing policy paper.
- The UK's National Risk Assessment of Proliferation Financing.
- Advisory notices issued by UK authorities.

The Firm should also be aware of the Home Office's Serious and Organised Crime Strategy last updated in November 2014.

The MLRs can be enforced by both criminal and civil penalties.

4.6.2 FCA Expectations

The FCA expects firms, including ARs, to follow the rules contained in the SYSC sourcebook, which are intended to drive an effective, risk-based approach. The SYSC provisions place emphasis on the detailed guidance contained within the Joint Money Laundering Steering Group's (JMLSG's) Guidance which supports firms in meeting their obligations to follow a risk-based approach under the UK AML/CTF regime. The FCA will take into account whether a firm has followed the provisions contained in the guidance. The Firm also recognises the FCA's Financial Crime Guide, which, along with the JMLSG guidance, is considered 'relevant guidance' as described in Regulations 76(6) and 86(2) of the MLRs 2017. Guidance is updated from time to time, so it is advisable to view guidance at source to ensure the latest version is being used.

The FCA's webpage on the MLRs covers the main aspects of the UK's anti-money laundering regime from a regulatory perspective.

The Firm must put in place and operate arrangements that enable it to comply with AML/CTF/CPF legislation. Kevin Gallacher is the senior manager responsible for operational systems and controls to prevent financial crime. Emma Jones is the MLRO. The MLRO is responsible for the oversight of the Firm's AML activities, and is the key person in the implementation of the Firm's AML/CTF/CPF strategies and policies. Gillian Gallacher, Partner and Compliance Officer, is the Firm's Deputy MLRO. **ARs' policies and procedures should incorporate/reflect the controls and roles at principal level.**

Money laundering risk is defined as the risk that a firm may be used to facilitate money laundering. Failure by a firm to manage this effectively will increase the risk to society of crime and terrorism. The MLRO is responsible for ensuring financial systems and controls are in place to take adequate notice of the risk of money laundering to which the business is exposed, and shall report to the partners regularly.

The Firm and its ARs are also required to mitigate the risk of terrorist and proliferation financing.

There is a high degree of commonality between the AML, CTF and CPF regimes. Indeed, the FATF's 40 recommendations cover all but 3 are specific to CTF (Recommendations 5, 6 and 8) and Recommendations 1, 2, 7 and 15 which have been expanded to also cover PF. As such, the AML measures firms put in place can also be used mitigate the risk of TF and PF. However, there are key differences between all 3, for example:

1. Often only small amounts needed to commit terrorist acts and moderate amounts used for proliferation activity, but large amounts often involved in money laundering.
2. Terrorism can be funded from legitimately obtained income.
3. Proliferation often involves state-sponsored programs.
4. Detection focus for proliferation is on individuals, entities, states, goods and materials and transactions often look like normal commercial activity, but structured to hide origin of funding. Whereas, money laundering typically involves a complex web of transactions often involving shell companies and offshore secrecy havens.
5. The money trails for TF and PT tend to be linear but ML money trails are often circular eventually ending up with the person who generated the funds.

Sources of information on TF and PF risks include: press reports; OFSI alerts; NCA alerts; FATF typologies; and court judgements.

4.6.3 AML Systems & Controls

SYSC 6.3.1 R requires the Firm to have in place systems and controls that:

1. Enable it to identify, assess, monitor and manage money laundering risk.
2. Are comprehensive and proportionate to the nature, scale and complexity of its activities.

SYSC 6.3.3 R requires the Firm to carry out regular assessments of the adequacy of its systems and controls.

In identifying its money laundering risk and in establishing the nature of its systems and controls, a firm should consider a range of factors, including:

1. Its clients, products and activity profiles.
2. Its distribution channels.
3. The complexity and volume of its transactions.
4. Its processes and systems.
5. Its operating environment.

The partners have assessed the Firm as being at low risk from a money laundering perspective for the following reasons:

- The Firm's business consists of providing investment management services to Professional Clients (funds) and not Retail Clients.
- The associated money laundering risks relate to the transfer and redemption of money/funds to and from the funds and from its ARs (monthly fee).
- The Firm's deals with low volumes of high value clients/funds and has an in-depth relationship with each client.
- The client take-on process involves a detailed understanding of the client's needs and priorities and anticipated inflows and outflows of funds in order to determine suitable investment parameters. The Firm usually maintains ongoing contact with its clients in order to review market developments and performance.
- Given the nature of the Firm's business, it expects to be remunerated by its clients for its services via bank transfers or cheques. It would be very unusual to receive cash payments or payments from unrelated third parties; and any such requests for payments will be subject to further enquiries.
- The Firm's client base is generally located in comparable jurisdictions with adequate AML standards.
- Any changes in the business are reviewed on a regular basis by the Compliance Officer and the risks are reconsidered.

ARs should carry out and document their own risk assessments.

Regulated firms are also required to undertake risk assessments prior to the launch of new products or business practices including in new jurisdictions, as well as new technologies. Firms should review risk assessments in response to material changes and developments.

4.6.4 Reporting Suspicions of Money Laundering

4.6.4.1 Main Obligations

Staff of the Firm and ARs must report any suspicious activities to the MLRO, whose responsibility it is then to determine whether or not a report should be made to the NCA. In the absence of the MLRO, this should be made to the Deputy MLRO. The Firm's staff may be disciplined if they fail without reasonable excuse to report potentially suspicious activity. Senior management of the Firm/ARs must permit the MLRO to:

1. Have access to any information in the Firm's/AR's possession that could be relevant.
2. Make a report without the approval of any other person.

4.6.4.2 The SAR Regime

- If a step that needs to be taken in a relevant transaction or matter would fall within sections 327 to 329 of POCA, the member of staff will need appropriate consent from the NCA before taking that step. 'Appropriate consent' is defined in section 335 of POCA. The MLRO should seek consent from the NCA at the same time as submitting the SAR.

- If NCA consent is needed, the member of staff must not take any further substantive action unless or until the consent is received and communicated to the member of staff by the MLRO. However, this will not prevent the staff member from progressing the matter otherwise (e.g. in writing letters or conducting searches), **provided they do not commit the tipping-off offence**.
- The initial notice period is **7 working days** from the day after receipt of the consent request. If the NCA refuses consent, the entity is subject to a moratorium period of 31 days, at which point deemed consent applies.
- The NCA can apply for 31-day extensions to the moratorium period of up to 186 days in total past the original 31-day period expiry date.
- The Criminal Finances Act (CFA) allows greater information sharing within the regulated sector, subject to the conditions set out below (from s339ZB of the POCA 2002) being satisfied, permitting one firm in the regulated sector to disclose information to another, whether or not requested to do so by the other firm, or on request or with the permission of the NCA. **Only the MLRO or Deputy MLRO can request disclosure and any disclosure requests must be sent to the MLRO/Deputy MLRO without delay**.
    - Condition 1 is where —
        a. A is carrying on a business in the regulated sector as a relevant undertaking.
        b. The information on which the disclosure is based came to A in the course of carrying on that business.
        c. The person to whom the information is to be disclosed (or each of them, where the disclosure is to more than one person) is also carrying on a business in the regulated sector as a relevant undertaking (whether or not of the same kind as A).
    - Condition 2 is that —
        a. An NCA authorised officer has requested A to make the disclosure or,
        b. The person to whom the information is to be disclosed (or at least one of them, where the disclosure is to more than one person) has requested A to do so.
    - Condition 3 is that, before A makes the disclosure, the required notification has been made to an NCA authorised officer (see section 339ZC(3) to (5)).
    - Condition 4 is that A is satisfied that the disclosure of the information will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.
    - A person may disclose information to A for the purposes of making a disclosure request if, and to the extent that, the person has reason to believe that A has in their possession information that will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.
    - The Act also sets out in s339ZC other conditions such as, the information the disclosure request must contain including that it must identify the person suspected of money laundering (if known) and the information it seeks, as well as details of the person who should receive the information. Where relevant, the request must also include the information the recipient firm would need in order to assess whether or not disclosing the information would meet the test of assisting in connection with a suspicion.
- The CFA enables the submission of joint/super SARs. However, whether or not to submit a joint/super SAR is the decision of the MLRO/Deputy MLRO. Staff members of the Firm and ARs should submit a SAR, as required, to the MLRO/Deputy MLRO in the first instance. For further information, please refer to the Home Office Circular issued in February 2018 on the sharing of information within the regulated sector, and between the regulated sector, the police and the NCA.
- The NCA can request further information from the person who made the disclosure, or any other persons in the regulated sector, following receipt of a SAR.

4.6.5 Government and International Findings

The Firm is required to obtain and act on findings issued by the UK government or an internationally accredited organisation of which the UK is a member, such as the FATF.

These findings will be published when the government, a government department or the FATF has examined money laundering prevention arrangements in a jurisdiction other than the UK and has found those arrangements to be materially deficient from relevant international and accepted standards. The FATF's latest (2018) Mutual Evaluation Report on the UK can be accessed here.

4.6.6 Risk-Based Approach

The Firm's risk-based approach categorises clients as either low, medium or high risk and requires the application of KYC measures and monitoring appropriate to the overall level of risk posed by the individual/entity. Whatever the approach taken, the broad objective is that prior to establishing a business relationship, the Firm/AR must know at the outset of the relationship:

- Who its customers and, where relevant, the controllers and/or beneficial owners of its customers, are.
- Where they operate.
- What they do.
- The source of their funds (the origin of the funds involved in the business relationship or occasional transaction).
- The source of their wealth (how they acquired their total wealth).
- Their expected level and type of activity.

The above analysis must be documented.

The Firm/AR must apply appropriate, risk-sensitive customer due diligence (CDD) measures on customers when it does any of the following:

- Establishes a business relationship.
- Carries out an occasional transaction.
- Suspects money laundering or terrorist financing.
- Doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification.

Where the client is a legal person, trust, company, foundation or similar legal arrangement, there is a specific requirement under the amended MLRs to take reasonable measures to understand the ownership and control structure of that client. Whilst beneficial ownership is clearly defined in the MLRs 2017, control is not. However, reference to Persons with Significant Control (PSC) information on Companies House is referred to. Therefore, PSC information and regulatory definitions of controllers should also be considered on a case-by-case basis.

The General Rule (Regulation 30(2) for the MLRs 2017) states that the verification of the identity of the client and, where applicable, the beneficial owners (and controllers), must, unless an exception applies, take place before the establishment of a business relationship or the carrying out of an occasional transaction.

The level of due diligence that is appropriate will depend on the level of risk posed by the prospective client taking into account numerous factors. The Firm should assess the risk posed by each client on a case-by-case basis, assigning appropriate weighting to relevant risk factors in order to produce an overall risk rating/profile for each client, having full regard to the high-risk factors contained in Regulation 33 of the MLRs 2017 (as amended in 2019). When weighting factors, the Firm should ensure:

- Weighting is not unduly influenced by just one factor.
- Commercial considerations do not inappropriately influence the risk assessment.
- Situations identified by national legislation or risk assessments as always presenting a high money laundering risk cannot be overruled by the Firm's weighting.
- The Firm is able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

Annex 4-II of the JMLSG Guidance Part 1 contains a fuller list of illustrative risk factors a firm may address when considering the money laundering/terrorist financing risk posed by customer situations, which is consistent with the Risk Factor Guidelines issued by the ESAs.

Section 5 of Part 1 of the JMLSG Guidance sets out how to properly verify the identity of different types of person. The UK government's webpage How to prove and verify someone's identity also contains some useful guidance.

Written records of all due diligence actions taken should be kept, especially where there have been difficulties in identifying beneficial owners, for at least 5 years from the end of the business relationship or from the date of the occasional transaction. See Regulation 28 (7) and (8) of the MLRs for more information on beneficial ownership requirements and difficulties.

Examples of clients/characteristics that are likely to fall within low, medium or high risk are listed in the following sections but each client should be judged on a case-by-case basis.

4.6.6.1 Low Risk

- Regulated financial institutions based in the UK; those located in EU, FATF or comparable jurisdictions.
- Government offices and agencies in all jurisdictions except for those in the non-cooperative countries and territories (NCCTs).
- Companies or their subsidiaries (50% or more) whose shares are traded on a UK or EU regulated market or equivalent exchange.
- Reputable, well-known organisations, with long histories in their industries or large market capitalisation and with substantial public information about them and their principals and/or controllers.
- Clients represented by those whose appointment is subject to court approval or ratifications (e.g. executors).

4.6.6.2 Medium Risk

All other clients that do not fall within either a low-risk category or a high-risk category including (but not restricted to):

- Subsidiaries of or entities associated with low-risk clients.
- Private companies from the UK, EEA or comparable jurisdiction provided they are not undertaking high-risk business.

In the absence of high-risk indicators the Firm's clients are expected to be private companies and individuals who will be categorised as medium risk.

For private companies the Firm/AR may obtain the following information from an independent source such as Companies House or from a reputable business information provider:

- An official document containing the client's full name and registered number.
- Evidence of client's registered office in the country of its incorporation.
- Evidence of client's business address.
- Its articles of association or other governing documents.

- Names of all directors or members of the management body.
- Names of all direct and indirect beneficial owners owning 25% or more of the entity.
- Names of any individuals who otherwise exercise control over the management of the company.
- Copy of latest audited accounts where available.
- Evidence of group ownership (e.g. sufficiently detailed structure chart), where relevant.
- The identity of at least one director must be verified via a certified passport or driving licence copy and a recent (dated within the last 3 months) utility bill or active bank account statement.

For clients that are individuals, the Firm/AR must obtain **and verify** their full name, residential address and date of birth and verify using a certified passport or driving licence copy and a recent (dated within the last 3 months) utility bill or active bank account statement.

If the client is a trust or charity, or another legal form, requirements in Part 1 of the JMLSG Guidance should be checked and if queries remain, the MLRO should be consulted to advise on the appropriate client take-on process.

4.6.6.3 High Risk – Requires Advance Approval from Compliance Officer or MLRO

To enable the Firm to consider the risks associated with high-risk clients in the context of its own risk appetite and risk management processes, and to confirm whether or not the risks are acceptable, a client categorised as high risk should be:

- Subject to appropriate, risk-sensitive *enhanced* due diligence measures, including ongoing monitoring where appropriate.
- Subject to adequate measures to establish and verify the source of wealth and source of funds.
- Signed off by the Firm's Compliance Officer or MLRO in advance of services being provided at both the Firm and AR level. Sign-off is provided, where appropriate, on the basis of a review of, and a discussion covering, a file note summarising all relevant risk factors and the complete file to ensure a holistic view is taken of the subject matter. Where the risk profile of a prospective or existing client (or investor or investee), either as part of initial due diligence or as a result of ongoing monitoring, is beyond the Firm's risk appetite, the Compliance Officer and MLRO will issue instructions on how to terminate the relationship. These instructions must be followed.

Examples of high-risk client types, or factors that separately or collectively indicate a client is high risk, are as follows:

- Relationships involving politically exposed persons (PEPs), their family members and/or known close associates:
    - A PEP is defined in the 2017 Regulations as 'An individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.'
    - The latest NRA judges wealth management (and private banking) firms to be particularly exposed to the risk of being used to launder the proceeds of political corruption and tax evasion.
    - Prominent public functions include:
        - Heads of state, heads of government, ministers and deputy or assistant ministers.
        - Members of parliaments or of similar legislative bodies.
        - Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances.
        - Members of courts of auditors or of the boards of central banks.
        - Ambassadors, charges d'affaires and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level).

        - Members of the administrative, management or supervisory boards of state-owned enterprises.
        - Directors, deputy directors and members of the board or equivalent function of an international organisation.
    - Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, e.g. a senior official at state level in a federal system, the Firm should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.
    - Family members of a PEP include:
        - A spouse or partner of that person.
        - Children of that person and their spouses or partners.
        - Parents of that person.
    - Close associates of a PEP include:
        - Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP.
        - Any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.
    - The Firm is not required to apply enhanced due diligence measures to family members or close associates of a PEP when the PEP is no longer entrusted with a prominent public function, whether or not the one-year period after the PEP has exited the position in question has expired.
    - Also see section 4.8.6.4 below, which covers the FCA's expectations of firms' treatment of PEP relationships.
    - The MLRs 2017 (as amended) require the UK to create and maintain lists of offices and functions that qualify as politically exposed at national level.
- Complex business ownership structures, such as offshore special purpose vehicles, that make it easier to conceal underlying beneficial owners, especially where there is no legitimate commercial rationale.
- Relationships involving clients that reside in or are nationals of NCCTs.
- Business relationships or transactions with high-risk third countries: the MLRs 2017 (as amended by the Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021) contain a list of countries considered high-risk in Schedule 3ZA (currently located here). The list will be periodically updated by way of further regulations, e.g. to reflect relevant changes to FATF lists. Therefore, relevant staff members of the Firm/AR must register for updates to keep pace with developments or check the list regularly but particularly as part of onboarding and ongoing monitoring.
- Accounts that involve large and/or regular payments to or from unrelated third parties.
- Where there is evidence of complex or unusually large transactions; or unusual patterns of transactions, which have no apparent economic or legal purpose – in these situations the Firm should as far as reasonably possible examine the background and purpose of the transactions and, should the relationship proceed, apply enhanced monitoring of the business relationship and include a higher degree of scrutiny over transactions.
- Names that have been previously linked with financial crime or other adverse media.
- Clients based in or conducting business in or through high-risk jurisdictions with known levels of corruption and/or organised crime, or drug production and distribution.
- Clients engaged in higher risk business activities.
- Companies issuing bearer shares, especially if incorporated in higher risk jurisdictions.
- Clients that have been subject to a suspicious transaction report.

- Clients that have not been physically present for identification purposes. This does not apply to clients to whom simplified due diligence applies (see below).
- A client that is the beneficiary of a life insurance policy.
- A client that is a third-country national seeking residence rights or citizenship in exchange for transfers of capital, purchase of a property, governments bonds or investment in corporate entities.
- Transactions without certain safeguards, for example, as set out in regulation 28 (19) concerning electronic identification processes.
- Transactions related to oil, arms, military defence, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or archaeological, historical, cultural and religious significance, or of rare scientific value.
- Transactions connected to controlled (see list here) or dual-use items, e.g. carbon fibre, vacuum pumps, electronic components, and testing equipment, which can also be used in the nuclear industry.

4.6.6.4 Politically Exposed Persons – FCA's Expectations of Firms

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates.

PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category.

In respect of PEPs, family members and associates of PEPs, enhance due diligence measures should always be applied and senior management approval will need to be obtained prior to acceptance of the relationship.

The risk presented by PEPs and their connected persons will not always be the same – some factors will mean the associated risk of one PEP is further up the high-risk scale than other PEPs and therefore more extensive checks should be conducted in these situations.

The Firm must take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship in order to allow the Firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity.

The measures the Firm should take to establish the PEP's source of wealth and the source of funds will depend on the degree of high risk associated with the business relationship, and where the individual sits on the PEP continuum. The Firm should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

See training presentation and FCA Guidance for more information on PEPs, including the risk factors to consider and the types of checks to perform.

4.6.6.5 Simplified Due Diligence

Simplified due diligence (SDD) is where, following a risk assessment, it is considered that there is a low risk of money laundering/terrorist financing/proliferation financing (ML/TF/PF) associated with the prospective client.

When assessing whether there is a low degree of risk of ML/TF/PF in a particular situation, and the extent to which it is appropriate to apply SDD measures in that situation, a firm must take account of at least the following risk factors:

- Whether the customer is:

- A public administration, or a publicly owned enterprise.
- An individual resident in a geographical area of low-risk credit or financial institution subject to the requirements in the 4th Money Laundering Directive.
- A company listed on a regulated market.
- An independent legal professional holding pooled accounts.
- Certain life assurance and e-money products (see Part II, sectors 7 and 3).
- Certain pension funds (see paragraphs 5.4.4 and 5.3.208ff).
- Child trust funds and junior ISAs.

Applying SDD might involve:

- Checking with the home country central bank or relevant supervisory body.
- Checking with another office, subsidiary, branch or correspondent bank in the same country.
- Checking with a regulated correspondent bank of the overseas institution.
- Obtaining from the relevant institution evidence of its licence or authorisation to conduct financial and/or banking business.

The Firm, therefore, must have reasonable grounds for believing that the customer falls within one of the categories set out below and maintain a record of this assessment, the initial due diligence and ongoing monitoring (where applicable) for at least 5 years following the termination of the relationship.

SDD may therefore be applied to the following categories of client/investment products:

- Certain other regulated firms in the financial sector.
- Companies listed on a regulated market.
- Beneficial owners of pooled accounts held by notaries or independent legal professionals.
- UK public authorities.
- Community institutions.
- Certain life assurance and e-money products.
- Certain pension funds.
- Certain low-risk products.
- Child trust funds.

SDD measures must not be applied, or continue to be applied, where:

- The Firm's risk assessment changes and it no longer considers that there is a low risk of ML/TF/PF.
- The Firm suspects money laundering or terrorist or proliferation financing.
- There are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identity or verification.

4.6.6.6 Standard KYC Evidence

Standard KYC evidence can be obtained for firms and individuals that do not meet the criteria for SDD but are not deemed to be higher risk clients, e.g. on a risk-assessed basis, private limited companies and private individuals.

Staff should also refer to the current version of the relevant training material and the template KYC and client categorisation checklist when assessing what information should be obtained from the customer.

Staff should refer to the Firm's KYC Process and Checklist and/or the JMLSG's Part 1 Guidance for a list of acceptable documents for other client types.

4.6.6.7 Enhanced Due Diligence (EDD)

The General Obligation in Regulation 33(1) is that EDD should be applied in any situation that presents a higher risk of money laundering or terrorist financing, or where the information obtained as part of its KYC process is insufficient in relation to the risks presented.

The extent of EDD must be commensurate to the risk associated with the business relationship or occasional transaction but firms can decide, in most cases, which aspects of CDD they should enhance. This will depend on the reason why a relationship or occasional transaction was classified as high risk.

It should be noted that EDD should always be applied to PEPs (including domestic PEPs) and their associated/connected persons. It should also be noted that EDD measures continue to apply to PEPs for a year after they have left office.

In addition to the general obligation referred to above, the MLRs 2017 prescribe 6 specific circumstances in respect of which EDD measures must be applied. These are:

- In any case identified by the Firm under its risk assessment (or in information provided by the supervisory authorities) where there is a high risk of ML/TF/PF.
- In relation to correspondent banking relationships (see JMLSG Guidance Part II, sector 16: Correspondent relationships).
- If a firm has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP.
- In any case where a customer has, or is suspected to have, provided false or stolen identification documents or information on establishing a relationship.
- In any case where:
    - A transaction is complex and unusually large.
    - There is an unusual pattern of transactions.
    - Transactions that have no apparent economic or legal purpose.
    - Transactions involving or connected to cryptoassets, controlled or dual-use items.
- In the case of business relationships or transactions involving high-risk third countries, the amended MLRs specifically require firms to apply one or more of the following enhanced CDD measures:
    - Obtaining additional information on the customer and on the customer's beneficial owner;
    - Obtaining additional information on the intended nature of the business relationship;
    - Obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
    - Obtaining information on the reasons for the transactions;
    - Obtaining the approval of senior management for establishing or continuing the relationship;
    - Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

4.6.6.8 Reliance on Third Parties

Where a firm relies on a third party to carry out CDD measures, it must obtain from the third party all the information needed to identify the customer or beneficial owner.

The Firm must enter into written arrangements with the third-party provider being relied on which:

- Enable the Firm to obtain from the third party immediately on request (or at the latest within 2 working days) copies of any identification and verification data and any other relevant documentation on the identity of the customer or beneficial owner.

- Require the third party to retain copies of the data and documents referred to above for 5 years beginning on the date on which the third party is relied on by the Firm.

There is nothing in the MLRs 2017 that prevents the Firm applying CDD measures by means of an appropriate agent or an outsourced service provider, as set out in the MLRs 2017, provided that the arrangements between the Firm and the agent or outsourced service provider provide for the Firm to remain liable for any failure to apply such measures and the agent or service provider agrees to be relied upon.

Whether a firm wishes to place reliance on a third party will be part of the Firm's risk-based assessment. In practice, the Firm needs to know:

- The identity of the customer or beneficial owner whose identity is being verified.
- The level of CDD that has been carried out.
- Confirmation of the third party's understanding of their obligation to make available, on request, copies of the verification data, documents or other information.

4.6.6.9 Reliance on Electronic CDD Measures

Regulation 28 of the MLRs set out the circumstances under which electronic identification processes may be considered in undertaking CDD measures. Specifically, where these are:

- Independent of the person whose identity is being verified.
- Secure from fraud and misuse.
- Capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.

See sections 5.3.39-5.3.53 of Part 1 of the JMLSG Guidance for more information on the use of electronic checks.

The Firm's view is that a combined approach of both electronic and manual checks will likely be appropriate in most cases given the Firm's typical client.

4.6.7 Beneficial Ownership

The 2017 Regulations state that a beneficial owner is normally an individual who ultimately owns or controls the customer on whose behalf a transaction is being conducted. In respect of private individuals the customer is the beneficial owner, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement on the Firm to make proactive searches for beneficial owners in such cases, but it should make appropriate enquiries where it appears that the customer is not acting on their own behalf.

The 2017 Regulations define beneficial owners as individuals either owning or controlling more than 25% of body corporates or partnerships or otherwise owning or controlling the customer. These individuals must be identified, and reasonable measures must be taken to verify their identities.

In relation to a trust, the ML Regulations define the beneficial owner as each of:

- The settlor.
- The trustees.
- The beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up or operates.
- Any individual who has control over the trust.

In relation to a foundation or other legal arrangement similar to a trust, the beneficial owners are those who hold equivalent or similar positions to those set out in paragraph 5.3.10.

In relation to a legal entity or legal arrangement which does not fall within 5.3.8-5.3.10, the beneficial owners are:

- Any individual who benefits from the property of the entity or arrangement.
- Where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates.
- Any individual who exercises control over the property of the entity or arrangement.

The threshold of beneficial ownership in the MLRs 2017 is 25%. The Firm/AR is required to obtain and hold adequate, accurate and current information on its own beneficial ownership. Authorities and firms should be able to access this information in a timely manner.

Trustees are required to disclose their status when becoming a client and are similarly required to make beneficial owner information available to authorities and firms.

Before establishing a business relationship, the identity of a client or beneficial owner must be verified using corresponding beneficial ownership registers, where available, or otherwise, on the basis of documents or information obtained from a reliable source which is independent of the client. The Firm/AR must take reasonable measures so that it is satisfied that it knows who the beneficial owner is. It is up to the Firm/AR to consider whether it is appropriate, in light of the money laundering or terrorist financing risk associated with the business relationship, to make use of records of beneficial owners in the public domain, ask its client for relevant data, require evidence of the beneficial owner's identity on the basis of documents or information obtained from a reliable source which is independent of the client, or obtain the information in some other way.

As risk dictates, the Firm/AR must undertake reasonable measures to understand the ownership (and control structure) of its customers and retain evidence of the steps taken on file.

Where a firm has not succeeded in identifying the beneficial owner, or is not satisfied that the individual(s) identified is (or are) in fact the beneficial owner(s), as well as that being a finding in itself which the firm should consider as part of its overall risk assessment, the amended Regulation 28 requires the firm to take reasonable measures to verify the identity of senior managing officials of the legal person in question.

Written records of all actions taken to identify beneficial owners and/or senior managing officials, and any difficulties in identifying the same, should be kept for at least 5 years from the end of the business relationship or the date of the occasional transaction.

4.6.7.1 Discrepancies in Registers and beneficial ownership

Subject to certain conditions/restrictions detailed in Regulation 30A of the MLRs, firms are required to report to Companies House (or the equivalent registrar) any discrepancies in PSC (persons with significant control) between the information they collect about a customer as part of initial due diligence before establishing a business relationship, or which becomes available to the firm when complying with the MLRs, and the information held by Companies House (or the equivalent registrar).

Guidance on how to report relevant discrepancies to Companies House can be found here.

From April 2023, the discrepancy reporting obligation is being expanded to the reporting of material discrepancies in beneficial ownership information arising from ongoing CDD obligations including for the Register of Overseas Entities.

4.6.7.2 Trusts

From 1 September 2022, the Regulation 30A of the MLRs will require firms to request proof of the trust's registration with, or an excerpt from, the Trust Registration Service (TRS) register from the client at the outset of the business relationship.

4.6.8 Ongoing Monitoring

Ongoing monitoring means scrutinising activity on a risk-sensitive basis or in certain situations (see below) to ensure that it is consistent with what the Firm/AR knows about its client and taking steps to ensure that the Firm's/AR's knowledge about the business relationship remains current.

Under Regulation 28(11), firms must conduct ongoing monitoring of the business relationship with their clients. The Regulation also states that ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, business and risk profile.
- Ensuring that the documents or information obtained for the purposes of applying CDD are kept up to date.

Part 1 of the JMLSG states that the essentials of a monitoring system, which can be real-time or after the event, manual or automated, are having up-to-date client information on the basis of which it will be possible to spot the unusual, and asking pertinent questions promptly to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious, and taking appropriate action on the findings.

Monitoring should be appropriate to the frequency, volume and size of transactions with clients in the context of the associated risks.

In accordance with Regulation 33(1), higher risk accounts and client relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring. FCG 3.2.9 provides examples of enhanced ongoing monitoring measures.

The Firm uses, and within 24 hours can gain access to, additional software to assist with enhanced ongoing monitoring. All higher risk relationships requiring senior management sign-off are added to the 'watchlist'.

4.6.9 Additional Notes on Client Risk Management

1. The Firm/ARs will not become party to a client relationship except with clients that have been identified in accordance with its own risk-based approach and, where applicable, have been approved by Firm/AR senior management.
2. The Firm/ARs will not do any business with clients of a dubious or criminal provenance.
    - In client relationships, the Firm/ARs will not proceed on the basis of mistrust; however, should the provenance of the client be subject to question or where doubts arise, additional clarifications are necessary before the business can take place.
3. The Firm does not participate in a transaction without an understanding of the economic context.
    - Understanding of the economic context can also include the identification of the financial beneficiary and the placing of the identification on the record if this is required for evaluating the consequences of a transaction.
4. The amended MLRs require the Firm/AR to examine the purpose and background of all transactions that fulfil at least one of the following conditions including to determine whether those transactions or activities appear suspicious:
    - They are complex,
    - Unusually large,
    - Conducted in an unusual pattern, and/or
    - They do not have an apparent economic or lawful purpose.

The Firm does not knowingly/actively accord support to illegal activities.

4.6.10 Cryptoassets

A recognised definition of cryptoasset is: 'A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically.'

Certain cryptoasset businesses are in scope of the MLRs 2017 (as amended), which means that they will be subject to the requirements of the MLRs, including to have policies, controls and procedures in place to manage ML and CTF risks, but also to register with the appropriate AML supervisor – the FCA.

The FCA has published a webpage explaining different aspects of the cryptoasset regime, including its registration process, supervisory approach and change in control requirements.

As highlighted by numerous bodies (including the FCA, FATF, G20) the main risks from cryptoassets are to: financial crime prevention, consumers and market integrity. There is also the potential for issues in cryptoasset markets to transfer to other markets.

FATF reports that virtual currencies are vulnerable to money laundering, terrorist and proliferation financing and provide for the circumvention of sanctions because they:

- Avoid the formal financial system.
- Allow greater anonymity than traditional payment methods.
- Make tracing more difficult.
- Can be traded on the internet with relative ease anywhere in the world with/through third parties that may not have any (obvious) physical real-world presence – this also exposes users to internet trading hacking risk.
- Generally involve non-face-to-face relationships.
- Have the potential to permit anonymous funding, including third-party funding through virtual exchanges that do not properly identify the source of funds.
- Have the potential to permit anonymous transfers if due diligence on sender and receiver is inadequate.
- Remain largely outside the scope of regulation in many jurisdictions, although virtual asset service providers (VASPs) are in scope of the MLRs in the UK and in many other jurisdictions.
- The absence of, or differences in, regulation and oversight means markets are exposed to traditional forms of manipulation and abuse.

Currently the main financial crime impacts for the Firm and its ARs from cryptoassets are where:

- An investor's source of funds/wealth is, or involves, cryptoassets – conduct risk-based due diligence taking into account the weak audit trail and the potential for cryptoassets to be used for, or to launder proceeds from, illicit activity.
- An investment is recommended in a cryptoassets firm – conduct risk-based due diligence, initially and on an ongoing basis (where the risk is considered high), including on the founders. As more jurisdictions publish their regulatory position on cryptoasset products and services, checking the regulatory status of firms involved in cryptoasset activities, and their degree of compliance with relevant rules, is essential.

Although investments in cryptoassets have been increasing as investors seek better potential returns than more traditional investments, cryptoassets activity remains relatively low in comparison to more traditional/main-stream forms of investment. Therefore, the Firm considers its risk from cryptoassets to be low. However, it has noted that the involvement of large businesses is increasing the popularity/use of cryptoassets, therefore, it will keep this risk assessment under review as the sector develops.

Where the Firm or an AR are considering becoming involved in cryptoassets space, the following best practice principles should be considered and implemented:

- Developing staff knowledge and expertise on cryptoassets to help them identify the clients or activities which pose a high risk of financial crime.
- Ensuring that existing financial crime frameworks adequately reflect the crypto-related activities which the Firm is involved in, and that they are capable of keeping pace with fast-moving developments.
- Understanding the control and ownership structures of cryptoasset firms before establishing a business relationship or conducting an occasional transaction.
- Engaging with clients to understand the nature of their businesses and the risks they pose.
- Carrying out due diligence on key individuals in the client business including consideration of any adverse intelligence.
- In relation to clients offering forms of crypto-exchange services, assessing the adequacy of those clients' own due diligence arrangements.
- For clients which are involved in initial coin offerings, considering the issuer's investor-base, organisers, the functionality of tokens (including intended use) and the jurisdiction.

4.6.11 Unexplained Wealth Orders

UWOs are orders issued by the High Court, subject to certain conditions – see below – being met, to authorised officers of appropriate supervisory authorities (e.g. FCA, NCA and HMRC) requiring the respondent to provide a statement that sets out the nature and extent of their interest in the property covered by the order, and requiring them to explain how they obtained the property. Where trustees of a settlement hold the property, the UWO may require details of the settlement. The explanation must include details of how any costs incurred in obtaining the property were met.

The UWO will set out the form and manner in which the statement should be given, whom it should be given to and where it is to be given or sent. It may be accompanied by a request to provide information or documents.

An agency applying for a UWO must apply to the court specifying or describing the property for which it is seeking the order and the person it thinks holds the property. UWOs are able to capture persons and property outside the UK.

The court will make the UWO if it is satisfied:

- The respondent holds the property and it is worth more than £50,000.
- There are reasonable grounds to suspect the respondent's known sources of legitimate income would not have been sufficient to enable the respondent to acquire the property.
- There are reasonable grounds for suspecting that the property has been obtained through unlawful conduct.
- The respondent is either a PEP, or family member/known close associate of a PEP, 'responsible officers' of the entity that owns the property, or there are reasonable grounds to suspect the respondent/someone connected to the respondent, is or has been involved in a serious crime anywhere in the world.

When applying to the court for a UWO, the relevant enforcement authority may apply at the same time for an interim freezing order which would prohibit the person receiving the UWO from selling it.

If the respondent fails (without a reasonable excuse) to comply with the UWO's requirements in the specified timeframe, then the property will become 'recoverable property' for the purposes of POCA.

It will be a criminal offence to knowingly or recklessly make a misleading statement when responding to a UWO and could be punishable by up to 2 years' imprisonment and/or an unlimited fine.

4.6.12 Interim Freezing Orders

POCA allows the High Court to make an interim freezing order in respect of any property that is the subject of a UWO, on the application of the relevant enforcement authority, if it thinks there is a risk a recovery order resulting from the UWO might otherwise be frustrated. Once made, the enforcement authority can apply for a receiver to be appointed.

4.7 Financial Sanctions

Financial sanctions are restrictions put in place by the UK government that limit the provision of certain financial services, or restrict access to financial markets, funds and economic resources, in order to achieve a specific foreign policy or national security objective. The Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act) provides the legal framework for the UK to impose, update and lift sanctions autonomously.

FATF recommendations target proliferation financing, as well as ML and TF, and require countries to implement targeted financial sanctions to comply with UN Security Council resolutions and also to criminalise the act. The UK's Counter Proliferation programme can be viewed here.

Financial sanctions come in many forms but the most common types of financial sanctions currently in use or used in recent years are:

- Targeted asset freezes, which are usually applied to named individuals, entities and bodies, restricting access to funds and economic resources.
- Restrictions on a wide variety of financial markets and services – these can apply to named individuals, entities and bodies, to specified groups or to entire sectors. To date these have taken the form of: investment bans; restrictions on access to capital markets; directions to cease banking relationships and activities; requirements to notify or seek authorisation prior to certain payments being made or received; and restrictions on provision of financial, insurance, brokering, advisory services or other financial assistance.
- Directions to cease all business of a specified type with a specific person, group, sector or country.

The Office of Financial Sanctions Implementation (OFSI, part of HMT) helps to ensure that financial sanctions are properly understood, implemented, and enforced in the UK. The Economic Crime (Transparency and Enforcement) Act 2022 has strengthened OFSI's powers.

All firms are required to comply with the UK's sanctions regime completely. Dealing with individuals/entities subject to sanctions is a criminal offence. The OFSI can also impose civil monetary penalties and publish details of breaches that have not resulted in a monetary penalty.

All clients, individuals and entities should be screened against the sanctions list as part of initial and ongoing KYC due diligence and evidence of screening should be placed on file. The lists are available here. If screening results in a match the Firm's Compliance Officer or MLRO should be notified and their instructions followed.

Specific exemptions or licencing grounds exist to enable certain future transactions to take place that would otherwise be prohibited. Licences can only be issued by OFSI (Office of Financial Sanctions Implementation) and it may attach conditions to licences. Licences cannot be issued retrospectively.

The most up-to-date version of the legislation that imposes a specific sanctions regime must always be referred to. These can be found here.

Staff within the Firm and ARs are advised to sign up to OFSI alerts. This can be done here.

For more information on sanctions, visit the OFSI website.

4.8 Bribery and Corruption

4.8.1 Introduction

In general terms, bribery is defined as giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly, or to reward that person for having already done so. Therefore this could cover seeking to influence a decision-maker by giving some kind of extra benefit to that person rather than by what can legitimately be offered as part of a tender process.

Transparency International (TI), a global organisation that works with governments, businesses and citizens to tackle corruption, defines corruption as 'The abuse of entrusted power for private gain.' TI explains that corruption can be further classified, according to the amounts of money lost and the sector in which it occurs, as:

- Grand corruption: 'Consists of acts committed at a high level of government that distort policies or the central functioning of the state, enabling leaders to benefit at the expense of the public good.'
- Petty corruption: 'Everyday abuse of entrusted power by low- and mid-level public officials in their interactions with ordinary citizens, who often are trying to access basic goods or services.'
- Political corruption: is the 'Manipulation of policies, institutions and rules of procedure in the allocation of resources and financing by political decision makers, who abuse their position to sustain their power, status and wealth.'

TI's website contains further information on corruption, including animated definitions of key terms in its Anti-Corruption Glossary.

The Bribery Act 2010, together with the Criminal Finances Act 2017 (see below), provides the legal framework to combat bribery and corruption. In the UK government's Anti-Corruption Strategy 2017-2022, the government outlines its continued commitment to making sure the UK financial sector, and the financial sectors of its Overseas Territories and Crown Dependencies, remain hostile to illicit finances.

The Bribery Act 2010 establishes 4 categories of offence:

1. Bribing another person (active bribery).
2. Being bribed (passive bribery).
3. Bribing a foreign public official.
4. Failure of a commercial organisation to prevent bribery on its behalf.

The first 3 offences are capable of being committed by an individual or a company but only a company can commit the fourth offence.

The Ministry of Justice has published Guidance for firms on how to prevent bribery by persons associated with them. Associated persons include agents, representatives, contract workers and some suppliers, as well as staff members.

A possible defence against the corporate offence of failing to prevent bribery is having effective measures in place to prevent bribery. These measures should be: risk based and proportionate; owned by senior

management; effectively communicated to staff and associated persons; and regularly monitored and reviewed.

ARs have the same exposure as the Firm under the Act for failing to prevent bribery by associated persons.

4.8.2 Anti-Bribery and Corruption Policy

The Firm operates a zero-tolerance approach to bribery and corruption and has an anti-bribery and corruption (ABC) policy in place (see Appendix L), which all members of staff and ARs are required to read, understand and comply with, and all other associated persons need to be aware of.

4.8.3 Anti-Bribery and Corruption Risk Assessment

The Firm's clients are typically UK-incorporated limited companies and UK-based LLPs, which are registered as ARs with the FCA. The ownership structure of its clients tends to be quite flat/non-complex and rarely involve individuals outside of the senior management. Where an AR is an LLP with a corporate partner, the directors/owners of the corporate partner are fully established.

It is noted that companies and limited partnerships (LPs), especially Scottish LPs, are particularly attractive to criminals due to the relative ease and low cost way in which they can be incorporated and dissolved, and that they are subject to few reporting and transparency obligations than other corporate forms .

To date none of the Firm's ARs are LPs. A number of funds managed by the Firm are structured as LPs but the Firm, as manager but also as principal for the fund advisers (ARs) is significantly involved in the set up and oversight of the funds. In addition, none of the Firm's ARs have been owned or controlled by a PEP or an organisation linked to a PEP.

The Firm only accepts introductions from known contacts and conducts thorough checks on prospective clients and their senior management regardless of the source of the referral, in accordance with its risk-based approach.

The Firm conducts enhanced due diligence in situations of higher risk and has strict guidelines, including a low approval threshold, for gifts and hospitality.

The Firm receives monthly reports on activities from its ARs and conducts a full routine monitoring visit at least every 12 months.

As such, the Firm considers its ABC risk to be low to moderate.

4.8.4 ABC Controls

The Firm has adopted the following controls to prevent bribery taking place – ARs should have similar controls in place:

- Clear, documented responsibility for reducing the risk of financial crime, including bribery and corruption. This responsibility rests with both the MLRO and Compliance Officer.
- Senior management understand and are informed of the bribery and corruption risks facing the Firm via the provision of management information addressing the financial crime risk.
- Senior management are required to review and approve, in advance, all higher risk relationships (such as those linked to a PEP or known close associate of a PEP).
- Remuneration structures are designed to avoid incentivising staff to gain business through bribes.
- Regular reviews of risk management by senior management which include the Firm's exposure to financial crime risk and the systems and controls in place to mitigate this risk.

- Risk-based approval for third-party payments and documentation demonstrating a clear understanding of the reason behind all payments.
- Where necessary, monitoring of any schedule of third-party payments (large payments, a large number of small payments, payments to connected parties, payments to political connections, high-risk jurisdictions, unusual, complex or secret payments).
- Countries regarded as higher risk in terms of bribery and corruption in accordance with the Transparency International Corruption Perception Index factored into risk assessments.
- Prohibiting provision of cash to staff (apart from de minimis amounts to cover small incidental expenses on an exceptional basis).
- Policy on gifts and incentives – see section 7 and Appendix L.
- Prohibition on the receipt or giving of cash gifts.
- Performing checks when recruiting new staff that are proportionate to their respective roles, e.g. criminal record checks.
- Providing staff with relevant, understandable and effective training.

4.9 Tax Evasion Facilitation

4.9.1 Introduction

The Criminal Finances Act 2017 (CFA) came into force on 30/09/17 and, amongst other things, comprises 4 parts:

- Part 1 – deals with proceeds of crime, money laundering, civil recovery, enforcement powers and related offences. It also creates a range of new powers for law enforcement agencies.
- Part 2 – ensures relevant money laundering and asset recovery powers will be extended to investigations under the Terrorism Act 2000 and the Proceeds of Crime Act (POCA) 2002.
- Part 3 – creates 2 new corporate offences of failure to prevent facilitation of tax evasion in the UK or abroad.
- Part 4 – contains minor and consequential amendments to POCA and other legislation.

The CFA follows on from the UK government's Action Plan for AML and CTF and key provisions are detailed below.

4.9.2 Corporate Failure to Prevent Tax Evasion

The CFA, amongst other things, contains 'failure to prevent' offences, similar to that in the Bribery Act 2010, in relation to tax evasion facilitation:

- Failure to prevent facilitation of UK tax evasion covers any offence of cheating the public revenue and any other fraudulent evasion of tax, thereby including duty and VAT fraud.
- Failure to prevent facilitation of foreign tax evasion captures conduct by an associated person that:
    - Amounts to an offence under foreign law.
    - Relates to a breach of duty relating to tax imposed under the law of that country.
    - Would be regarded by the courts of any part of the UK as amounting to being knowingly concerned in, or in taking steps with a view to, the fraudulent evasion of that tax.

Facilitation offences include aiding, abetting and inchoate offences (e.g. incitement).

As with the corporate offence under the Bribery Act, the new CFA offences are on a legal entity basis. Therefore, **ARs have the same exposure as the Firm under the Act for failing to prevent the facilitation of tax evasion by associated persons**.

The following 3 stages apply to both offences and each stage must be satisfied:

- Criminal tax evasion by a taxpayer (either an individual or a legal entity) under existing law.
- Criminal facilitation of the tax evasion by an 'associated person' of the relevant body acting in that capacity.
- Failure of the relevant body to prevent its representative from committing the criminal facilitation act.

It should be noted that there is no requirement for the Firm to have benefitted from the facilitation to commit the offence.

The offences cover all 'relevant bodies', including bodies corporate and partnerships, **wherever** formed, but not natural persons.

A person is 'associated' with a relevant body if that person is a staff member, agent or other person who performs services for or on behalf of the relevant body. The question as to whether a person is performing services for or on behalf of an organisation is intended to be broad in scope and is determined by reference to all the relevant circumstances. Therefore associated persons are likely to include: staff members at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

For the corporate offence to be committed there must be criminal facilitation of the taxpayer by a person acting in the capacity of a person associated with the relevant body (stage 2). The associated person must deliberately and dishonestly take action to facilitate the taxpayer-level evasion. The UK offence does not radically alter what is criminal; it simply focuses on who is held to account for acts contrary to current criminal law.

Additional requirements apply to the foreign offence, as it is narrower in that only relevant bodes with a UK nexus can commit it and 'dual criminality' applies – where there are equivalent offences at both the taxpayer and associated person facilitation levels in the relevant overseas jurisdiction and the actions of both the taxpayer and facilitator would be offences under UK law.

HMRC has produced guidance to assist firms in the prevention of tax evasion. The guidance states the following, which helps explain the scope of the new law relating to the new offences:

'The legislation aims to tackle crimes committed by those who act for or on behalf of a relevant body. The legislation does not hold relevant bodies to account for the crimes of their customers, nor does it require them to prevent their customers from committing tax evasion. Nor is the legislation designed to capture the misuse of legitimate products and services that are provided to customers in good faith, where the individual adviser and relevant body did not know that its products were intended to be used for tax evasion purposes.'

The Act provides firms with a defence that if, at the time the offence was committed, they had in place 'A system of reasonable procedures that identified and mitigated tax evasion facilitation risks, then prosecution is unlikely.' (Source: HMRC Guidance)

As with the Bribery Act guidance, the CFA guidance is centred around 6 principles/key actions:

1. Conduct a risk assessment.
2. Implement proportional risk-based procedures.
3. Obtain and demonstrate top-level commitment form.
4. Conduct sufficient due diligence.
5. Communicate the Firm's approach and procedures, including from senior management and through appropriate training.
6. Monitor and review the Firm's policy and relevant procedures at least annually.

The guidance also contains illustrative examples of the different types of procedures that would be relevant for various types of companies. For example, timely self-reporting will be viewed as an indicator that a relevant body has reasonable procedures in place.

The penalties for facilitating tax evasion will include unlimited financial penalties and ancillary orders such as confiscation orders.

The key considerations for senior managers of corporate entities are as follows:

- What are my responsibilities under the new legislation?
- How can I discharge them?
- How are procedures implemented and documented?
- How often are they tested?

4.9.2.1 Risk Assessment

The Firm typically has no more than 15 limited companies incorporated in the UK and/or UK-based LLPs that are registered as ARs with the FCA. Directors and partners of ARs are required to be FCA Approved Persons. ARs and their Approved Persons are therefore required to be fit and proper for the duration of their relationship with the Firm and for as long as they hold Approved Person status.

The Firm and its ARs are only able to deal with Professional Clients and Eligible Counterparties, which can include high net worth individuals classed as Elective Professional Clients.

For a small number of fund clients the Firm also acts as the AIFM or delegated sub-manager. In these situations the Firm's responsibilities include approving fund subscriptions.

At any time the Firm's associated persons may include the following – those marked with an asterisk are considered potential sources of tax evasion facilitation risk:

- Individuals approved as CF30s under the Firm or Certified staff at Firm level.*
- Other staff members, partners or agents of the Firm or its ARs.*
- Gem Compliance Consulting Ltd (Gem) and staff members/agents of Gem.*
- Its accounting firm.*
- Its legal advisers.*
- Back-office function providers, including: (virtual) office space providers; Dropbox (cloud-based file storage provider); Office 365; IT consultants; online training platform(s); newsletter platform.
- Third-party professional connections (entities and individuals) that occasionally provide business referrals to the Firm on an informal, zero-remuneration basis.

Although the Firm operates in the financial services sector, which is considered by HMRC as a higher risk sector in respect of tax evasion, for the following reasons the Firm believes the risk that an associated person could facilitate tax evasion is low-medium:

- Its typical clients (ARs) are seen as relatively low risk from a financial crime perspective.
- Activities on its behalf are conducted predominantly in the UK and non-UK activity is largely within relatively low-risk jurisdictions.
- The Firm uses reputable businesses that undertake to comply with, inter alia, strict codes of practice, and their staff are required to maintain their competence in many areas including financial crime.
- The Firm's lawyers and accountants, whilst potentially higher risk associated persons, are firms covered by their own professional regulation, including their own financial compliance regimes.
- The transactions the Firm is directly involved in are not overly complex and are considered sufficiently transparent.
- The parties involved in the transactions are well known to the Firm.

- It has appropriate agreements in place with all clients and associated persons (with the exception of those that make informal business referrals to the Firm).
- Third-party business referrals to the Firm are from well-known contacts and no reliance is placed on any due diligence conducted by, or assurances from, the introducer. (See standard AR selection procedure for more information.)
- The senior management of its clients are all Approved Persons subject to the FCA's FIT criteria – see earlier section for a description of this.
- The FCA's Principles for Businesses apply to the Firm and its ARs.
- Fund clients use well-known, reputable firms, which are subject to the same/equivalent financial crime regulations/legislation as the Firm, to assist them in structuring and administering the funds, including conducting detailed KYC on underlying investors, which in some cases the Firm is required to approve beforehand.

Although the risk is seen as low-medium the potential risk that does exist primarily stems from the Firm's ARs and Approved Persons, as they are seen as an extension of the Firm for regulated activities, and Gem, which operates many of its back-office processes, including AR and Approved Person pre-application due diligence.

4.9.2.2 Risk Mitigation

- Robust AR selection and onboarding procedures.
- On the Firm's behalf, and in accordance with the Firm's operational procedures, Gem conducts extensive pre-application due diligence on prospective ARs and their senior management teams before submitting applications to the FCA for appointment/approval.
- Clear and regular AR training programme, which includes financial crime training and covers the CFA specifically.
- Issuance of relevant ad hoc guidance to ARs covering topics such as incentives and performance management.
- Clear zero-tolerance policy on tax evasion prevention, which has been approved and communicated to all clients and associated persons of the Firm by the Firm's Managing Partner.
- Other relevant policies and procedures include those relating to:
    - AML, CTF and CPF, risk-based due diligence in particular.
    - Gifts, benefits and hospitality.
    - Fraud.
    - Remuneration.
    - Whistleblowing.
- Request details of the CFA policies/stance of associated persons, where applicable, as part of the Firm's initial due diligence.
- Relevant clauses in terms and conditions, including contracts for services, service agreements, and subscription agreements – require natural and legal persons to take all relevant steps to prevent the facilitation of tax evasion.
- Template KYC and client categorisation checklist contains:
    - Zero-tolerance statement.
    - Requirement to conduct tax-related due diligence.
- Allocation of responsibility for ensuring front-line compliance with the procedures by clients to one of the Firm's partners (Kevin Gallacher).
- Proportionate scrutiny of bank details for payments to/from clients, associated persons and underlying investors.
- Where structures include an overseas element the rationale for this should be checked and documented. Where the rationale is tax-related documentary evidence confirming the legitimacy

of the structuring, and compliance with relevant laws, from appropriately qualified persons is required.

4.9.2.3 Red Flags and High-Risk Indicators

Higher risk situations and possible signs of tax evasion are similar to those for fraud, and AML/CTF, so AML/CTF processes and procedures are relevant to preventing/spotting tax evasion. Other possible signs include:

- Overly complex company structure(s) covering a number of jurisdictions without sufficient supporting information to justify the structure(s).
- Difficulty in establishing UBOs and reluctance to provide requested information.
- A lifestyle (as evidenced from internet searches and social media) that is not commensurate to the declared income and wider information provided to date.
- Difficulty in establishing source of wealth and/or funds.
- Payments made to/from third-party accounts with no obvious, or at best a tenuous, connection to the individual/entity.
- Failure to provide details of their registration with HMRC's Affluent Unit (for those subject to UK revenue and customs laws and with net wealth of between £2.5m and £20m).
- Unusual activity on bank statements that could be suggestive of 'off the book' deals.
- Multiple transactions of buying and selling within a Group between subsidiaries and often across jurisdictions, including known tax havens (see list below), without a clear commercial reason for operating such a complex model.

HMRC has published a report outlining the use of tax avoidance schemes in the UK, which can be accessed here.

See also Part 1 of the JMLSG Guidance, which can be accessed here, for high-risk factors that can also apply to tax fraud – Annex 1 – jurisdictions, and Annex II – Customers.

According to a news report, the following jurisdictions are the biggest enablers of global corporate tax abuse:

- The Cayman Islands
- British Virgin Islands
- Bermuda
- Luxembourg
- Netherlands
- Hong Kong
- Singapore
- United Arab Emirates
- Jersey
- Switzerland

The background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose should be examined as far as is reasonably possible.

If a member of staff becomes suspicious, they should send a SAR along with all relevant supporting documentation, to the Firm's MLRO without delay. The staff member should ensure they do not alert the subject to the filing of a report and await further instructions from the MLRO before proceeding further.

5a APPROVED PERSONS

5a.1 Introduction

In March 2016, the FCA implemented the Senior Manager & Certification Regime (SM&CR) for UK banks, building societies, credit unions, and dual-regulated investment firms. This replaced the Approved Persons regime for those entities.

The SM&CR was implemented on 9 December 2019 to all solo directly regulated firms including Midmar, although ARs are not in scope and remain on the existing arrangements as specified below until advised further.

Under SYSC 5.1.1, principal firms require their ARs to employ personnel with skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.

As an authorised firm, the Firm is required to have systems and controls to satisfy itself of the suitability of individuals within ARs that will require FCA approval.

An individual's honesty and competence assessment will be made at the point of recruitment taking into account the level of responsibility the individual will assume in the Firm. This will also be assessed for existing staff if there is any reason to consider that this has changed since appointment or where the Firm chooses to carry out a regular confirmation exercise.

Where the person may be performing a Controlled Function (as defined by FCA rules at SUP 10A), the individual may need to be FCA pre-approved to carry out that role before the activities start.

When considering the fitness and propriety (FIT) of Approved Persons specifically, 3 main criteria are considered which are:

- Honesty, integrity and reputation (FIT 2.1).
- Competence and capability (FIT 2.2) – see Chapter 11 of the Manual for further detail.
- Financial soundness (FIT 2.3).

5a.2 Approved Persons and Controlled Functions

There are currently a number of Controlled Functions (not all of which are relevant to all ARs) and, prior to any individual performing any of these functions, they must be approved to do so by the FCA. These are listed at SUP 10A.4 and application to ARs is clarified at SUP 10A.1.15 - 16.

Relevant Controlled Functions for ARs may include some of the following which will also depend upon the type of legal entity involved.

Significant Influence – FCA Governing Functions

CF 1 (AR):	Director Function (for a limited company AR).
CF 2 (AR):	Non-Executive Director Function.
CF 3 (AR):	Chief Executive Function - only if relevant (for limited companies and for a managing partner LLP).
CF 4 (AR):	Partner Function (for an LLP AR).
CF 5 (AR)	Director of Unincorporated Association Function.

Customer-Dealing Function

CF 30 (AR): Customer Function (for ARs performing this role).

5a.3 CF 30 – Customer Function

The FCA register for the Firm and separately the Compliance Officer maintains a list of Approved Persons and roles for its ARs. If an individual is unsure whether they are an Approved Person, including whether this is for the Customer Function, they should contact the Compliance Officer to clarify this.

With regard to the CF 30 Customer Function, it is imperative that an individual holds this function before undertaking any of the following relevant activities otherwise this will be a breach of FCA rules:

- Advising on investments other than non-investment insurance contracts (but not where this is advising on investments in the course of carrying on the activity of providing basic advice on a stakeholder product) and performing other functions related to this such as dealing and arranging.
- Giving advice to clients solely in connection with corporate finance business and performing other functions related to this.
- Dealing, as principal or as agent, and arranging (bringing about) deals in investments other than a non-investment insurance contract with or for, or in connection with customers where the dealing or arranging deals is governed by COBS 11 (Dealing and Managing) (**not available to ARs**).
- Acting in the capacity of an investment manager and carrying on functions connected to this (**not available to ARs**).

All Approved Persons are required to adhere to the FCA rules detailed in the FCA Handbook, specifically those relating to fitness and propriety.

5a.4 FIT Assessment

Assessment of the fitness and propriety of anyone to be performing a Controlled Function will include many of the following steps, (which are non-exhaustive) and prior to submission of an application by the Firm:

- Complete employment history (months and years) for the last 10 years (where applicable).
- Residential address information for the last 3 years (months and years).
- Verified ID (identify and address).
- Full CV (including clarification on any gaps of employment).
- Independent employment references for at least the last 6 years, satisfying SYSC 22 on regulatory references, where applicable.
- Pre-disclosure of any history which could impact the FCA's assessment of the candidate's fitness and propriety including investigative or disciplinary action by previous employers.
- Outside interests in an official capacity, i.e. directors or partners of other entities.
- Background due diligence checks completed by the Firm's compliance function including general internet searches, Companies House searches, credit history checks and criminal records checks.

5a.5 APER – Statements of Principle and the Code of Practice for Approved Persons

To help determine whether or not a person's conduct complies with the Statements of Principle, the FCA issued the Code of Practice for Approved Persons. Approved Persons need to comply with Principles 1-4 if they are approved to undertake Controlled Function 30, and Principles 1-7 if they are approved to undertake Controlled Functions 1-29.

Principles 1 – 4

1. An Approved Person must act with integrity in carrying out their accountable function.
2. An Approved Person must act with due skill, care and diligence in carrying out their accountable function.
3. An Approved Person must observe proper standards of market conduct in carrying out their accountable function.
4. An Approved Person must deal with the FCA and with other regulators in an open and co-operative way and must disclose appropriately any information of which the FCA would reasonably expect notice.

Principles 5 – 7

5. An Approved Person performing an accountable higher management function must take reasonable steps to ensure that the business of the firm for which they are responsible in their accountable function is organised so it can be controlled effectively.
6. An Approved Person performing an accountable higher management function must exercise due skill, care and diligence in managing the business of the firm for which they are responsible in their accountable function.
7. An Approved Person performing an accountable higher management function must take reasonable steps to ensure that the business of the firm for which they are responsible in their accountable function complies with the relevant requirements and standards of the regulatory system.

The FCA places considerable emphasis on the attainment and maintenance of competence with reference to all roles undertaken by Approved Persons.

It is of extreme importance that staff are familiar with these principles if they are an FCA Approved Person as breaking them can result in disciplinary action against them personally. If the FCA considers an Approved Person's misconduct to be sufficiently serious it can also ask for their 'approval' to be withdrawn and they would no longer be eligible to work in that Controlled Function.

The Compliance Officer maintains a record of all Approved Persons and details of the Controlled Functions they are permitted to undertake. Should an individual believe that they require approval, or that their circumstances change either in relation to personal details or fitness or propriety, they should discuss this as soon as possible with the Compliance Officer.

In order to perform a Controlled Function a completed Form A: 'Application to perform Controlled Functions under the Approved Persons regime' must be submitted to the FCA prior to a person undertaking such activities and confirmation of approval obtained. The most up-to-date version of this form must be used.

If a person ceases to perform a Controlled Function it is company policy that a completed Form C: 'Notice of ceasing to perform Controlled Functions' must be submitted to the FCA no later than 7 calendar days after an Approved Person ceases to perform that Controlled Function, and certainly no later than 10 business days (in accordance with SUP 10A.14.8). A notification to the FCA is required as soon as practicable where an issue regarding fitness or propriety has arisen.

If an Approved Person has a change in personal details including title, name and National Insurance number, or the person is absent for more than 12 weeks but is expected to return to the same role, it is company policy that this must be notified to the FCA within 7 calendar days of the Firm becoming aware of the event, and certainly no later than 7 working days (in accordance with SUP 10A.14.15). This is done by completing Form D.

All such notifications and applications must be done by the Firm using the FCA's Connect system of which the Compliance Officer is the principal user and the Compliance Manager and compliance associates, including junior associates, are additional users.

5b SENIOR MANAGERS & CERTIFICATION REGIME

5b.1 Introduction

The SM&CR applies to all FCA solo and dual-regulated firms authorised under the Financial Services and Markets Act 2000 (FSMA), as well as EEA and third-country branches. Firms that are not authorised under FSMA (for example payment services firms) are not covered by the SM&CR.

SM&CR applies to the Firm but does not apply to ARs, who continue to be subject to the Approved Persons regime (see Chapter 5A).

The FCA has provided a guide for solo-regulated firms.

There are 3 key parts to the SM&CR regime:

1. The Senior Managers regime.
2. The Certification regime.
3. Conduct Rules that apply directly to all staff within an in-scope firm except ancillary staff (e.g. cleaners, receptionists, etc).

The SM&CR aims to reduce harm to consumers and strengthen market integrity by creating a system that enables firms and regulators to hold people to account. As part of this, the SM&CR aims to:

- Encourage staff to take personal responsibility for their actions.
- Improve conduct at all levels.
- Make sure firms and staff clearly understand and can clearly demonstrate the allocation of responsibilities/ business areas amongst senior personnel.

Please refer to Appendix A of this Manual for a list of Senior Managers and Certified individuals at the Firm.

PART 1 – THE SENIOR MANAGERS REGIME

5b.2 Types of SM&CR Firm

What firms are required to do under the SM&CR depends on whether they are classified as 'limited scope', 'core', or 'enhanced'. Most firms will be core, however there are a small number of firms that would be regarded as a limited scope (due to the nature of activities that they perform) or enhanced. Core firms could move to enhanced firm status if the size of their organisation meets one of 6 criteria based on a size threshold. Further details are available in the FCA's guide for solo-regulated firms on when this could apply.

Midmar is classified as a core firm.

5b.3 Senior Manager Functions

Senior Manager Functions (SMFs) are held by the most senior people in a firm with the greatest potential to cause harm or impact upon market integrity. As with the previous Controlled Function regime, an SMF holder needs to be approved by the FCA before they can start their role. An exception to this is under the 12-week rule, where a person may cover for a Senior Manager without being approved, where the absence is temporary or reasonably unforeseen, and the appointment is for less than 12 consecutive weeks. However, for an individual to continue to perform the function(s) after 12 weeks, FCA approval of the individual for the function(s) in question needs to have been received.

A person may hold more than one SMF role and a single application can be used to apply for more than one SMF, e.g. SMF1, CEO and SMF16 Compliance Officer. A single Statement of Responsibilities per SMF is also acceptable. However, the FCA will consider the candidate's suitability for each function separately. If an individual is applying for an additional SMF role, although a Short Form A may be applicable, the FCA will review the competencies for the new responsibilities in isolation of existing approval(s).

The SMFs applying to a firm will depend on whether the firm is limited scope, core or enhanced. For a UK-based core firm such as Midmar, the SMFs that apply are as follows and some (SMF3, SMF27) will depend upon whether the entity is a limited company or partnership.

Brief description of function	Function number
Governing functions	
Chief Executive Function	SMF1
Executive Director Function	SMF3
Chair of the Governing Body Function	SMF9
Partner Function	SMF27
Required functions	
Compliance Oversight Function	SMF16
Money Laundering Reporting Function	SMF17

One point to note about SM&CR, is that it does not require firms to change their governance structure or hire new people to fill specific roles. SMFs only apply if a particular role is already performed by an individual or the SMF is a required function that a firm must have in place as set out in the rules.

5b.4 Duty of Responsibility

Every Senior Manager has a duty of responsibility under s.66 of FSMA. This means if something goes wrong in an area that a Senior Manager is responsible for, the FCA will consider whether the Senior Manager took reasonable steps to stop this from happening. In other words, if a firm breaches any FCA requirement, the Senior Manager responsible for that area could be held accountable if they did not take 'reasonable steps' to prevent or stop the breach.

In July 2018, the FCA published a Policy Statement (PS18/16) – Final Guidance: the duty of responsibility for insurers and FCA solo-regulated firms. The guidance states, amongst other things, that under the duty of responsibility, Senior Managers are accountable for their individual contributions to collective decisions and their implementation insofar as they concern any of the firm's activities for which they are responsible.

The burden of proof will lie with the FCA to show that the Senior Manager did not take the steps a person in their position could reasonably be expected to take to avoid the firm's breach occurring. Therefore, it is advisable for Senior Managers to ensure they create and maintain clear audit trails to demonstrate what action they took, when and why. If a Senior Manager is in any doubt about what action would be considered reasonable, the Senior Manager is advised to seek appropriate guidance, such as from the Compliance Officer.

When deciding whether to take action against someone based on the duty of responsibility, the FCA will look at all of the circumstances of the case. This will include the seriousness of the breach, the person's

position, responsibilities and seniority, and the need to use enforcement powers effectively and proportionately (as set out in the FCA's Decision Procedure and Penalties sourcebook (DEPP)). The FCA states that sometimes it will be appropriate to take action against a Senior Manager, sometimes against a firm, and sometimes against both. These decisions will be made on a case-by-case basis, applying the criteria set out in DEPP.

5b.5 Fitness and Propriety

Senior Managers (and also Certification staff and non-executive directors (NEDs)) must be fit and proper for their role and firms must employ/contract with personnel with the skills, knowledge and expertise necessary for the proper discharge of responsibilities allocated to them. When considering the fitness and propriety of these persons, the 3 main criteria considered are:

- Honesty, integrity and reputation.
- Competence and capability.
- Financial soundness.

The FCA sourcebook FIT sets out the guidance for these criteria.

Extra evidence collection over and above the Firm's standard requirements may be needed in certain situations, such as when assessing new candidates for these positions. Guidance on these additional evidential requirements is contained in the FCA's SM&CR guide for solo-regulated firms. The table below (from this FCA guide) summarises some of these requirements.

Summary of fitness and propriety requirements

	New hire	Internal hire (including intra-group hires)	Annual assessment
Senior Manager			
Regulatory reference	✓	✗	✗
F&P assessment	✓	✓	✓
FCA approval before commencing role	✓	✓	✗
Criminal record check	✓	✓	✗
Certification Function			
Regulatory reference	✓	✗	✗
F&P assessment	✓	✓	✓
Certificate for function	✓	✓	✓

5b.5.1 Criminal Record Checks

For Senior Managers and NEDs, there is a mandatory requirement to conduct a criminal record check as part of the approval process for that role. This applies to both external applicants and existing staff applications. Although not a requirement for Certification Functions, the Firm may choose to conduct these checks as it sees fit where they are legally allowed to do so.

The Firm conducts standard criminal record checks on individuals applying for Senior Manager roles and basic criminal record checks on Certification staff.

5b.5.2 Regulatory References

Another check that is required for new externally hired Senior Managers, Certification Functions and NEDs is a regulatory reference in line with the template under SYSC 22 Annex 1. The Firm has its own template based on this. Under this requirement, firms need to request from past employers, from the past 6 years, information relating to disciplinary action in relation to Conduct Rule breaches, and any findings that the person was not fit and proper. Firms providing a reference are also required to disclose any other information that may be relevant to assessing whether a candidate is fit and proper (e.g. number of complaints) covering the previous 6 years (unless it relates to serious misconduct, in which case there is no time limit).

Firms should use the FCA's standard regulatory reference template as a basis for sharing information.

Firms will also need to update regulatory references where new, significant information comes to light. Therefore, firms will need to keep a clear record of the regulatory references it has previously provided.

The Banking Standards Board has issued guidance on regulatory references, which the Firm will consider when providing a regulatory reference.

It is important to note however, that a record of the disciplinary action in this context only applies from when SM&CR was introduced for solo-regulated firms on 9 December 2019.

To ensure appropriate oversight for regulatory references, the Firm will have in place a Senior Manager with Prescribed Responsibilities (a & b) covering this area – see 5.7 below.

5b.6 Statement of Responsibilities

Each SMF holder is required to have an individual Statement of Responsibilities (SoR) clearly setting out their role and responsibilities. It is recommended these are signed, dated reviewed at least annually. A SoR should set out what they are responsible and accountable for, but not how they carry out those responsibilities. In addition, a SoR must be self-contained and not refer to other documentation. The FCA has published guidance on their expectations of such statements, FG19/2, and the Firm follows this guidance in its approach to its SoRs.

For persons with more than one SMF role, only one SoR is required, but this must detail and describe all the responsibilities held under these roles clearly and succinctly.

The SoR will need to be submitted to the FCA when applying for a Senior Manager to be approved. SoRs also need to be kept up to date and resubmitted to the FCA when there's a significant change to a Senior Manager's responsibilities (see SUP 10C.11 for guidance on what is considered a significant change).

5b.7 Prescribed Responsibilities

The FCA has set out specific Prescribed Responsibilities (PRs), defined in SYSC 24 of the Handbook, relating to key conduct and prudential risks where accountability must be assigned. These PRs are in addition to the inherent responsibilities that are an essential part of a Senior Manager's role. These PRs will also be captured within a Senior Manager's SoR.

PRs only apply to core and enhanced scope firms, and not limited scope firms.

Each PR should be given to the Senior Manager who is the most senior person responsible for that area or activity. This is again where the FIT rules apply in that the Senior Manager must have the appropriate level of knowledge and competence to undertake the responsibility properly.

A key point to note is that whilst assigning a PR to a Senior Manager does not require FCA approval, moving a PR from one Senior Manager to another Senior Manager will require an updating of these managers' SoRs, and these in turn must be submitted to the FCA for recording.

PRs should not be shared or divided between Senior Managers. If these situations are unavoidable then the Firm will need to demonstrate why this is justified and that no gap is left. SoRs for the Senior Managers involved must clearly explain how the responsibilities are shared or split, but accountability will remain jointly held.

The PRs for a core firm are as follows:

Handbook PR ref	Description
(a)	Responsibility for the firm's performance of its obligations under the SMR, including implementation and oversight.
(b)	Responsibility for the firm's performance of its obligations under the Certification Regime.
(b-1)	Responsibility for the firm's performance of its obligations in respect of notifications and training of the Conduct Rules.
(d)	Responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime.
(z)	Responsibility for the firm's compliance with CASS (if applicable).
Authorised fund managers (AFMs) only	
(za)	Responsibility for an AFM's assessments of value, independent director representation and acting in investors' best interests.

Due to the Firm's activities, responsibilities (z) and (za) do not apply to the Firm.

PART 2 – THE CERTIFICATION REGIME

5b.8 Overview

The Certification Regime covers specific functions that are not SMFs but may still have a significant impact on customers, the Firm, and/or market integrity. Details of the Certification Regime are found in the Handbook under SYSC 27. Those performing Certified roles do not require approval from the FCA, instead firms must ensure that individuals are and remain fit and proper to fulfil role requirements. These individuals should also have the necessary qualifications, and have completed, or are undergoing, relevant training. All of this needs to be checked and certified by the Firm at least annually.

Whilst there is no prescribed format to the certificates that a firm must issue to Certified staff, the certificate should make clear that the authorised firm is satisfied that the individual is a fit and proper person to perform a Certification Function. The certificate should also set out the aspects of the firm's business in which the individual will be involved.

An individual may hold more than one Certification Function. Where this is the case, a firm must assess the fitness and propriety of that person to carry out each function and the necessary competencies to do so. However, this can be done as a single assessment.

5b.9 Certification Functions

The Certification Regime only applies to employees of firms, individuals seconded to the firm and contractors, but it does not apply to NEDs, for example. The following table sets out the various Certification Functions that apply or could apply to the Firm. However, there are other functions that are captured in the Certification Regime firms as defined in SYSC 27.7. Certified staff should be added to the FCA's Directory of Certified Persons, via Connect.

	Certification Function	Description
1.	Significant Management Function	This function applies to firms that have personnel in place who, whilst not Senior Managers, are responsible for areas of the business, which due to their size, nature or impact, are considered significant by the firm. • The size and significance of the firm's business in the UK. • The risk profile of the business area. • The business area's contribution to the firm's capital requirements. • Its contribution to the profit and loss account. • The number of employees, Certification Functions or Senior Managers in the business area. • The number of customers served by the business area.
2.	The client dealing function	This function applies to any person dealing in or arranging investments with clients, including Retail and Professional Clients and Eligible Counterparties. This will include: • Financial advisers. • People who are involved in corporate finance business. • People who are involved in dealing or arranging deals in investments. • Investment managers. This does not include individuals who have no scope to choose, decide or reach a judgement on what should be done in a given situation, and whose tasks do not require them to exercise significant skill.
3.	Functions subject to qualification requirements	The full list is set out in the FCA's T&C sourcebook, but includes mortgage advisers, retail investment advisers, and pension transfer specialists.
4.	Supervisors or managers of a Certified Function, who are not a Senior Manager	This will make sure that people who supervise Certified employees are held to the same standard of accountability. It also makes sure a clear chain of accountability between junior Certified employees and the Senior Manager ultimately responsible for that area. For example, if a firm employs a customer-facing financial adviser, every manager above them in the same chain of responsibility will have to be certified (until the Senior Manager approved under the SMR is reached).

5b.10 Senior Managers and Certification Functions

Senior Managers who perform a Certification Function will also have to be certified if this role largely differs from the role they do as a Senior Manager. This is considered most relevant in relation to the Client Dealing Certification Function and where such individuals used to be CF30 approved advisers. In this situation a combined fitness and propriety assessment may be carried out which covers the requirements for both roles.

PART 3 – THE CONDUCT RULES

5b.11 Overview of the Conduct Rules

The Financial Services (Banking Reform) Act 2013 updated FSMA 2000 to give the FCA new powers to write Conduct Rules and apply them to all employees – not just Senior Managers or Certified individuals – within all authorised firms in a staggered roll-out spanning a number of years. The Conduct Rules are 9 enforceable rules that set basic standards of good personal conduct in relation to employees' performance of functions in the carrying on of activities by an in-scope firm such as Midmar. The FCA will use the Conduct Rules as a measure against which they can hold people to account. The rules can be found in the COCON chapter of the FCA Handbook.

As the Conduct Rules apply to staff directly, they are intended to, and will hopefully help, shape the culture, standards and policies of firms as a whole and promote positive behaviours that reduce harm from the top down and the bottom up.

They represent a meaningful change in the standards of conduct the FCA expects from those working in the industry, and by applying the Conduct Rules to a broad range of staff the FCA's aim is to improve individual accountability and awareness of conduct issues across firms. Conduct Rules apply to all firms, i.e. enhanced, core and limited scope firms.

5b.12 Application of the Conduct Rules

Application of the Conduct Rules is across a firm's regulated and unregulated financial services activities (including any related ancillary activities, i.e. an activity carried on in connection with a regulated activity). This differs from the FCA Statements of Principle and Code of Practice for Approved Persons, which applies only to regulated activities.

The Conduct Rules specifically apply to:

- All Senior Managers.
- All Certified Functions.
- All NEDs who are not Senior Managers.
- All other employees, except ancillary staff (i.e. people who do not perform a role specific to financial services – see below).

In this case, the FCA has adopted a broad definition of employee, which extends beyond the traditional employment law definition of the term to include secondees, as well as contingent and temporary workers. However, there is an exception for those performing specified ancillary functions such as receptionists, security staff, cleaners and catering staff, (where their role would be the same whether this is at a financial services firm or not), who are not subject to the Conduct Rules. At the Firm, Conduct Rules are deemed to apply to all members of staff.

5b.13 Conduct Rules Tiers

There are 2 tiers of Conduct Rules in place. The first tier applies to all relevant employees, but the second tier rules only apply to Senior Managers. The rules are set out in the following table together with the Handbook COCON reference:

First tier - Applies to ALL employees – Individual Conduct Rules COCON 2.1	
1	Act with integrity.
2	Act with due skill, care and diligence.
3	Be open and co-operative with the FCA and other regulators.
4	Pay due regard to the interests of customers and treat them fairly.
5	Observe proper standards of market conduct.
Second tier - Senior Managers only Conduct Rules COCON 2.2	
SC1	You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
SC2	You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system.
SC3	You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.
SC4	You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.

Examples of behaviour that the FCA considers could breach the rules are included at COCON 4.1 for all staff and COCON 4.2 for Senior Managers.

For UK firms, the Conduct Rules apply in 2 situations. They apply to activities carried out from the UK. They also apply to activities carried out from outside the UK, but only if the activity involves having contact with UK clients. This means that if a person based overseas does not deal with UK clients, the Conduct Rules will not apply to them.

Firms are also required to train relevant staff on how the Conduct Rules apply to their role and a Senior Manager must be allocated the PR for this. This should be done as part of induction for new staff and at least annually for existing staff. If a breach of the Conduct Rules becomes apparent, the Senior Manager must ensure this is notified to the FCA.

To ensure the effective operation of these processes, firms must put in place procedures to comply with Conduct Rules training and breach reporting requirements, which is a Prescribed Responsibility.

6 REGULATORY CAPITAL AND LIQUIDITY

6.1 Introduction

This section of the Manual sets out the Firm's arrangements to maintain adequate capital resources. This reflects the Firm's prudential supervision under the Investment Firms Prudential Regime (IFPR) from January 2022 as a small and non-interconnected (SNI) firm.

6.2 Overall Financial Adequacy Rule (OFAR)

The Firm has been categorised as an SNI firm. On that basis, the Firm comes under the rules in the MiFIDPRU Prudential Supervision sourcebook.

The Firm must at all times hold own funds and liquid assets which are adequate, both as to their amount and quality, to ensure that the Firm is able to remain financially viable throughout the economic cycle, with the ability to address any material potential harm that may arise from its ongoing activities, and that the Firm's business can be wound down in an orderly manner, minimising harm to consumers or to other market participants. This is known as the overall financial adequacy rule.

Essentially, the Firm must have capital resources to meet its liabilities as they fall due, and additionally have processes, strategies and systems to assess and maintain adequate (financial, capital, internal capital) resources to withstand the risks it is exposed to, and to meet all regulatory obligations.

6.3 Responsibility for Maintaining Adequate Capital Resources

The Compliance Officer in conjunction with any other partner(s) is responsible for monitoring capital resources and capital requirements and ensuring that there are sufficient capital resources.

6.4 Ongoing Capital Resources Requirement

As an SNI firm, the rules in MiFIDPRU state that ongoing capital must be comprised of an own funds requirement and a liquid assets requirement.

The own funds requirement is further comprised of a firm's permanent minimal capital requirement (PMR) under MiFIDPRU 4.4 and its fixed overheads requirement (FOR) under MiFIDPRU 4.5. The Firm's PMR is £75,000, subject to any transitional arrangements that apply on own funds as an existing firm prior to the implementation of IFPR.

A firm's FOR is an amount equal to one quarter of the firm's relevant expenditure during the preceding year. The accounting framework applied must accord with the criteria set out in MiFIDPRU 4.5.2R and set out at 6.10.1 below.

6.5 Annual Operating Expenditure

The Firm's relevant expenditure is defined as follows:

'The sum of the amounts described as total expenditure in the 4 quarterly financial returns up to (and including) that prepared at the firm's most recent accounting reference date, less the following items (if they are included within such expenditure)'.

- Staff bonuses, except to the extent that they are guaranteed, and other variable remuneration.
- Employees' and partners' shares in profits, except to the extent that they are guaranteed.
- Other appropriations of profits.
- Non-recurring expenses from non-ordinary activities.
- Shared commission and fees payable, which are directly related to commission, and fees receivable, which are included within total revenue.
- Interest charges in respect of borrowings made to finance the acquisition of the Firm's readily realisable investments.
- Interest paid to customers on client money (not applicable).
- Interest paid to counterparties.
- Fees, brokerage and other charges paid to clearing hours, exchanges and intermediate brokers for the purposes of executing, registering or clearing transactions.
- Taxes where they fall due in relation to the annual profits of the firm.
- Other expenses to the extent that their value has already been reflected in a deduction from own funds under MiFIDPRU 3.3.6R (Common equity tier (CET) 1 deductions).

FOR should be based on the last audited accounts. However, if the FOR increases by 30% or more during the year, this must become the new FOR requirements under the ICARA with immediate effect. If the FOR reduces by the same, FCA consent to reduced capital requirements must be obtained in advance.

A firm's financial resources requirement will be recalculated annually when its fourth financial return is prepared. The Firm must maintain financial resources sufficient to meet its new financial resources requirement from the date on which the fourth quarterly financial return is prepared and no later than 80 business days after the Firm's accounting reference date. The above FOR applicable at the accounting reference date will be based on the 4 quarterly financial returns prepared up to and on that date.

6.6 Liquid Assets Requirement

The basic liquid assets requirement for a firm equates to an amount of core liquid assets (defined in MiFIDPRU 6.3) which is equal to the sum of:

- One third of the amount of its FOR; and
- 1.6% of the total amount of any guarantees provided to clients.

The Firm normally holds its liquid funds requirement in cash.

6.7 ICARA

The Compliance Officer in conjunction with any other partner(s) is responsible for making sure that the OFAR is met. The Firm will utilise the internal capital adequacy and risk assessment (ICARA) process to identify whether it complies with the OFAR. This process is laid out in MiFIDPRU 7.

The ICARA is central to a firm's risk management process to identify and monitor the potential harms to consumers, to the market in which it operates and to the firm itself, and to reduce all potential material harms that may result from the ongoing operation of its business or from winding down.

Under FCA requirements, it covers:

- Identification, monitoring and mitigation of harms (in line with MiFIDPRU7 Annex 1).
- Business model planning and forecasting.
- Recovery and wind-down planning – assessing the adequacy of financial resources.

This will normally include a firm-wide Risk Register. The outcome may include holding additional own funds and liquid assets, where necessary.

The ICARA process should be reviewed at least once every 12 months but also to review this following any material change including an increase in costs. More complex firms might need to consider half yearly.

6.8 FCA Notification Requirements

Rules require that FCA investment firms must notify the FCA where their level of own funds and/or liquid assets fall below these intervention points.

The Firm needs to consider any notification impacts if own funds fall to within 110% of the requirement. Therefore, it is always recommended to hold more than 110% of the FOR and have additional surplus to avoid notification risk.

6.9 ARs and Capital Adequacy

ARs are not themselves subject to specific capital adequacy risks. However, the Firm as principal is required to ensure the financial soundness of its ARs in line with SUP 12 Annex 1. The Firm does this as part of onboarding a new AR but also on an ongoing basis through monthly reporting, receipt of at least quarterly management accounts from its ARs, and again as part of formal annual monitoring visits.

6.10 Financial Reporting

Principle 4 requires firms to maintain adequate financial resources. By submitting regular data, firms enable the FCA to monitor their compliance with Principle 4 and their prudential requirements in the FCA Handbook.

6.10.1 Electronic Reports

The Firm's required financial returns, as an IFPRI SNI, are showed at MiFIDPRU 9. The Firm's reporting schedule is listed on the FCA reporting system known as RegData. This normally requires the submission of quarterly financial statements based on the Firm's accounting reference date which is 31 March. In addition, annual audited financial statements must be sent to the FCA within 80 business days of its financial year end.

6.10.2 Submission of Data Items

When submitting the completed data item, except where there is no standard format, the Firm must use the format of the data item set out in MiFIDPRU9 Annex 1.
https://www.handbook.fca.org.uk/form/mifidpru/MIFIDPRU%209%20Annex%201R%20Data%20items%20for%20MIFIDPRU%209%20Annex%201R.pdf

Four guidance notes for completion of the data items are contained in MiFIDPRU9 Annex 2.
https://www.handbook.fca.org.uk/form/mifidpru/MIFIDPRU9_Annex2G_01012022.pdf

Sterling is the normal reporting currency; however, the systems permit reporting in the currency of the annual accounts.

Any non-standard format items must be sent to:

Central Reporting
The Financial Conduct Authority

12 Endeavour Square
London E20 1JN

Or via email to: Regulatory.reports@fca.org.uk

Copies of each submission should also be retained on the Firm's own records.

7 CONDUCT OF BUSINESS (COBS) – GENERAL

This chapter covers general COBS issues that apply to the Firm and its ARs.

7.1 Acting Honestly, Fairly and Professionally

COBS 2.1.1 R requires that all members of staff, within the Firm and its ARs, act 'honestly, fairly and professionally in accordance with the best interests of its clients'. This is known as the client's best interests rule.

7.2 Information Disclosure Before Providing Services

COBS 2.2A.2 R requires that the Firm and its ARs must provide certain information to a client before it conducts investment business for that client. This includes: information about the Firm itself and the services it is authorised to provide, investment strategy, risk warnings, execution venues (where applicable), and the charges the Firm makes for providing these services.

7.3 Inducements

COBS 2.3A applies to MiFID, equivalent third-country and Article 3 firm business, whilst COBS 2.3 applies to all other business. The rules in both sections require the Firm and its ARs not to receive or pay fees or commissions (monetary or in kind) unless these are disclosed and clear to the client and do not in any way impair the Firm's/AR's compliance with the client's best interests rule. Any such inducements should ultimately be to enhance the services that the Firm/AR can give its clients. The fees and/or commissions received must be reasonable in terms of the value of the service being provided. Records of inducements must be kept for at least 5 years.

7.3.1 Personal Gifts and Benefits

The Firm/ARs must take reasonable steps to prevent it, or any person acting on its behalf, from:

- Accepting or offering any inducements or
- Directing or referring any actual or potential business to another person on its own initiative,

if it is likely to conflict with any responsibility the Firm has toward its clients. In this regard, staff members are specifically reminded of the FCA's Principle 6 – customers' interests, which requires the Firm to pay due regard to the interests of its clients and treat them fairly.

The Firm/ARs must also adhere to the Firm's anti-bribery and corruption policy (Appendix L).

7.4 Agent as Client

COBS 2.4.1 R allows the Firm and its ARs to take instructions from agents acting on behalf of their own client. If the Firm or an AR is aware that a person with or for whom it is conducting permitted designated investment business is acting as agent for another person in relation to that business, then the agent is the client of the Firm/AR in respect of that business, if:

- The agent is another regulated Firm or an overseas financial institution, or

- The agent is any other person, provided that avoidance of the duties which the Firm would otherwise owe to the client is not the main purpose of the arrangements between the parties, UNLESS
- The Firm has agreed with the agent in writing to treat the agent's client as the Firm's client.

Please note that the Firm and its ARs are still required to treat the agent's client as their client for the purposes of AML Regulations.

7.5 Reliance on Others

COBS 2.4.4 R allows the Firm/ARs to rely on information provided to the Firm/ARs by another firm that is a MiFID investment firm, a third-country investment firm or a firm that has equivalent relevant requirements. The Firm/AR may also rely on information provided by others if it is satisfied the information can be relied on. However, the Firm/AR will retain ultimate responsible for satisfying any relevant requirements.

7.6 Client Categorisation

COBS 3.1.1 R requires the Firm to take reasonable steps to establish whether a new client is a Retail Client, Professional Client or an Eligible Counterparty. COBS 3.3.1 R requires the Firm to confirm, in writing, to the client before providing any services the client categorisation it has selected, detailing any limitations to the level of client protection that such a categorisation would entail compared with alternative categorisations. The Firm must also advise a client of their right to opt for a client category affording them a higher level of protection (COBS 3.3.1A UK, COBS 3.7.1 R). Opting for categorisation taking into account a client's knowledge and experience is considered below.

The Firm is authorised by the FCA to undertake regulated activities with or for Professional Clients and Eligible Counterparties only. It is therefore important that before the Firm or an AR acts for a client the client's correct categorisation is established. The Firm and ARs must maintain client categorisation records for a period of at least 5 years (COBS 3.8.2 R) from last activity.

The Firm's clients consist of its ARs, the funds the Firm manages and those funds' investors.

7.6.1 Retail Client

COBS 3.4.1 R states that a Retail Client is a client who is not a Professional Client or an Eligible Counterparty. **Neither the Firm nor ARs are permitted to deal with or for Retail Clients**.

7.6.2 Professional Client

COBS 3.5.1 R states that a Professional Client is a client who is a Per Se Professional Client or an Elective Professional Client.

7.6.2.1 Per Se Professional Client

COBS 3.5.2 R states that a Per Se Professional Client is a Professional Client that is not an Eligible Counterparty and is one of the following:

- Credit institution.
- Investment firm.
- Other authorised or regulated financial institution.
- Insurance company.
- Collective investment scheme or the management company of such a scheme.
- Pension fund or the management company of a pension fund.

- Commodity or commodity derivatives dealer.
- Local authority.
- Other institutional investor.

Or in relation to MiFID Business or Equivalent Third-Country Business, a large undertaking meeting 2 of the following 3 size requirements on a company basis:

- Balance sheet total of Euro 20m.
- Net turnover of Euro 40m.
- Own funds of Euro 2m.

7.6.2.2 Elective Professional Client

COBS 3.5.3 R states that the definition of an Elective Professional Client is a Professional Client that the Firm/AR has chosen to treat as an Elective Professional Client, and who has agreed to be classified as such and who complies with the COBS 3.5.3 R (1), (2) and (3), or in the event of undertaking non-MiFID business for that client COBS 3.5.3 R (1) and (3).

Essentially, where the Firm/AR wishes (and the client agrees) to categorise a client as an Elective Professional Client, e.g. a Retail Client, the Firm/AR is obliged to satisfy itself to a reasonable extent that the client concerned:

- Has the expertise, knowledge and experience with regard to the financial instruments and/or service proposed and that the client is, therefore, capable of understanding the impact of their decisions and of the inherent risks involved (**the qualitative test**).
- Has stated, in writing, that they wish to be classified as a Professional Client in respect to the services and/or financial instruments contemplated.
- Has received a clear written warning from the Firm/AR regarding the protections and investor compensation rights they should expect to lose that would otherwise be afforded to them as a Retail Client, and they have separately in writing acknowledged and accepted this.
- Is able to meet, in the event of undertaking MiFID Business, 2 of the 3 following **quantitative tests**:
    - The client has carried out transactions, in significant size, on the relevant market at an average frequency of 10 per quarter over the previous 4 quarters.
    - The size of the client's financial instrument portfolio, defined as including cash deposits and financial instruments, exceeds EUR 500,000.
    - The client works or has worked in the financial sector for at least one year in a professional position which requires knowledge of the transactions or services envisaged.

Under COBS 3.5.4R, if the client is an entity, the **qualitative** test should be performed in relation to the person authorised to carry out transactions on its behalf.

As clients of the Firm, ARs are not required to be Professional Clients. However, they would typically qualify. Funds will normally qualify as Per Se Professional Clients. A fund's investors will need to confirm via the Professional Client notice whether it is a Per Se or Elective Professional Client.

7.6.3 Eligible Counterparty

COBS 3.6.1 R. An Eligible Counterparty Client is either a Per Se Eligible Counterparty or an Elective Eligible Counterparty. The Firm may only undertake Eligible Counterparty business (dealing on own account, execution of orders on behalf of clients, reception and transmission of orders or ancillary services as per MiFID Annex 1 B) for an Eligible Counterparty and may not, therefore, undertake investment advice or investment management.

7.6.3.1 Per se Eligible Counterparty

COBS 3.6.2 R. A Per Se Eligible Counterparty is an Eligible Counterparty that the Firm has chosen to categorise as such and does not provide investment advice or investment management and is an entity as defined in COBS 3.6.2 R (1) to (10).

7.6.3.2 Elective Eligible Counterparty

COBS 3.6.4 R. An Elective Eligible Counterparty is an Eligible Counterparty the Firm has chosen to categorise as an Elective Eligible Counterparty and is an entity that is listed at COBS 3.6.4 R (1) and (2).

7.6.4 Providing Clients with a Higher Level of Protection

COBS 3.7.1 R provides a client the right to be treated in such a way that higher levels of protection are afforded. A client that the Firm categorises as a Professional Client or Eligible Counterparty could request to be classified as a Retail Client, or in the case of an Eligible Counterparty as a Professional Client. However, as the Firm cannot act for Retail Clients, if such protection was requested, the Firm would need to decline to act.

7.6.5 Policies, Procedures and Records

COBS 3.8.1 R requires the Firm to have appropriate written internal policies and procedures to categorise its clients.

COBS 3.8.2 R requires the Firm to keep records of the client's category, evidence of despatch of notice of categorisation sent to the client and a copy of the agreement entered into by the client. These records must be kept by the Firm for a minimum of 5 years after the client ceases to be a client of the Firm (COBS 3.8.2 R (3)(c)). As noted earlier, the Compliance Officer will keep all client records for a minimum of 5 years.

The above rules also apply to ARs.

7.7 Communicating With Clients Including Financial Promotions

7.7.1 Introduction

Section 21 of FSMA imposes a restriction on the communication of financial promotions by unauthorised persons. A person must not, in the course of business, communicate an invitation or inducement to engage in investment activity (a financial promotion) unless:

- They are an Authorised Person (a firm with a Part 4A, i.e. a directly authorised firm) or
- An Authorised Person approves the content of the financial promotion.

The Compliance Officer is ultimately responsible for authorising the Firm's financial promotions. However, the review and approval, where appropriate, of financial promotions has been generally delegated to competent individuals within the Firm with experience of COBS 4 rules.

There is no restriction on the media of communication to which the FCA requirements on financial promotions apply, and they therefore include printed materials, personal visits or telephone calls, and internet or other electronic media communications such as posts on blogs and Twitter.

The rules in the Handbook on communicating with clients and financial promotions are contained in COBS 4.

7.7.2 Fair, Clear and Not Misleading

COBS 4.2.1 R requires the Firm to ensure any communications with existing and potential clients must be 'fair, clear and not misleading'. Financial promotions addressed to clients must also be identifiable as such, except for a third-party prospectus where this relates to the Firm's MiFID business.

The Firm should ensure that a financial promotion:

1. For a product or service that places a client's capital at risk makes this clear.
2. That quotes a yield figure gives a balanced impression of the short and long term prospects for the investment.
3. That promotes an investment or service whose charging structure is complex, or in relation to which the Firm will receive more than one element of remuneration, includes the information necessary to ensure that it is fair, clear and not misleading and contains sufficient information taking into account the needs of the recipients.
4. Names the FCA as its regulator and, if it refers to matters not regulated by the FCA, makes clear that those matters are not regulated by the FCA.
5. That offers packaged products or stakeholder products not produced by the Firm, gives a fair, clear and not misleading impression of the producer of the product or the manager of the underlying investments.

7.7.3 Investment and Non-Independent Research

The Firm does not produce, arrange for the production of, publish or distribute its own investment research to clients or any other third party.

ARs may issue investment research or non-independent research and should refer to COBS 12 which includes requirements on disclosures and conflicts of interest. The Firm should review and approve any research prior to publication or dissemination.

COBS 12.2.22 R allows the Firm and its ARs to disseminate investment research produced, published and disseminated by other authorised firms not associated with the Firm or an AR unless the publisher of that investment research has expressly prohibited its further dissemination.

7.7.4 Direct Offer Financial Promotions

COBS 4.7.1R deals with direct offer financial promotions, which are promotions from firms, or on behalf of firms, that either propose to or invite from a respondent, an offer to enter into a controlled agreement with the firms. In relation to MiFID business a controlled agreement includes an agreement to carry on an ancillary service.

The Firm's policy is to prohibit the issue of direct offer financial promotions.

7.7.5 Promotions of Unregulated Collective Investment Schemes

Under section 238(1) of FSMA, a Firm must not communicate an invitation or inducement to participate in an unregulated collective investment scheme. Certain exceptions from this restriction are set out in FSMA (Promotion of Collective Investment Schemes) (Exemptions) Order 2001.

COBS 4.12.3R states that a firm may communicate financial promotions of unregulated collective investment schemes (defined as non-mainstream pooled investments (NMPI)) without breaching the provisions of section 238(1) of FSMA so long as the Firm only makes these financial promotions where it has made reasonable efforts to ensure these are only being made to permitted clients as detailed in Table COBS 4.12.4(4)R.

The marketing targets relevant to the Firm and its ARs are, typically:

- Category 2: Certified high net worth individuals.
- Category 4: The Firm's staff members and partners or its former staff members and partners or their immediate family.
- Category 7: Professional Clients or Eligible Counterparties.
- Category 8: Certified sophisticated investors.
- Category 9: Self certified sophisticated investors.

Before issuing such a financial promotion, the Firm/AR must have made a reasonable assessment, and be able to evidence such an assessment that this financial promotion is only to be issued to individuals where they have evidence, or it is reasonable to assume, that a particular exemption will apply. The assessment should also include the reasons for the outcome that subsequently results. (COBS 4.12.5).

Any financial promotions to such persons who are not clients of the Firm or its AR should be approved by the Firm's Compliance Officer or otherwise delegated to individuals who have experience of approving such items.

Where a financial promotion is exempt under categories 2, 8 or 9, this exemption can only be satisfied where there is an appropriate declaration obtained from the client in accordance with the requirements at COBS 4.12.6 – 4.12.11.

The Firm/AR must, when categorising persons with a view to a financial promotion of the unregulated collective investment scheme being communicated, at the time, make a record that demonstrates the basis that the Firm/AR has made reasonable attempts to ensure that the financial promotion is only being communicated to those persons eligible to receive such promotions.

7.7.6 Social Media Communications

If duties require individuals to speak on behalf of the Firm/AR in a social media environment, they must undergo training before doing so, seek prior approval for each communication and abide by the principles and guidelines set out below.

Likewise, if Firm/AR staff are contacted for comments about its organisation for publication anywhere, they should not respond without written approval.

7.7.6.1 Social Media Principles

- Take time to get to know the environment and the target audience/network.
- Be respectful, thoughtful and polite at all times.
- Be clear on who will be able to view the posts before they are being made.
- Err on the side of caution, if unsure, do not post it and/or discuss with line manager before doing so.
- Look out for security threats.
- Do not make promises or guarantees.
- Use alternative channels to handle complex/confidential queries and provide bespoke guidance/advice.
- Do not respond impulsively, take time and hold back if in any doubt.

7.7.6.2 Guidelines for Safe and Responsible Use of Social Media

- Individuals should be aware that they are personally responsible for all communications, which will be published on the internet for anyone to see.

- If affiliation with the Firm/AR is disclosed on personal social media profiles or in any social media postings, individuals must state that their views do not represent those of the Firm (unless they are authorised to speak on their behalf).
- Individuals should ensure that personal profiles and any content posted are consistent with the professional image presented to clients and colleagues.
- Individuals should consider the FCA's social media guidance, which includes examples of compliant and non-compliant practices, prior to making any posting (see key-point summary below and FG15/4).
- Communication with direct competitors should be approved in advance and kept to a minimum.
- When sharing content published on another website, use sharing buttons or functions provided by the website.
- If social media content that disparages or reflects poorly on the Firm or an AR is seen, the Compliance Officer should be contacted without delay.

7.7.6.3 FCA's Social Media Guidance (FG15/4) – Key Points

- Certain tweets are seen as non-real-time promotions – see Article 7 of the Financial Promotion Order 2005.
- Communications could amount to financial promotions if they include an invitation or inducement to engage in financial activity.
- All communications should be clear, fair and not misleading.
- Twitter communications can reach a large audience very quickly so this should be considered before tweeting and tweets should be appropriately and specifically targeted.
- If the tweet meets the definition of a financial promotion the standard financial promotion rules and principles apply – see relevant sections of this Manual and relevant training presentation – including approval by a competent individual within the authorised firm.
- Consider whether any risk warnings/disclaimers are required perhaps via an image to minimise impact on word-count and to ensure important messages are sufficiently clear.
- The firm from where a posting originates remains ultimately responsible for the communication therefore this should be considered when creating it.
- Staff should have regard to other applicable rules relating to promotions and marketing, such as those concerning unsolicited promotions, e.g. Privacy and Electronic Communications Regulations 2003.
- Consider what the most appropriate format for the communication is.

7.7.7 Approving Financial Promotions

COBS 4.10.2 R requires the Firm/AR to ensure that financial promotions are approved by the Firm, as an Authorised Person, before use. The Firm's policy is that it will aim to review each financial promotion within 5 working days from receipt. Please note that timescales for data rooms may be longer depending on volume. The Firm's Compliance Officer is ultimately responsible for approving all financial promotions. However, the review and approval, where appropriate, of financial promotions has been generally delegated to competent individuals within the Firm with experience of COBS 4 rules.

The Firm maintains a file of all final versions of all financial promotions together with relevant paperwork (e.g. completed checklists, where appropriate, emails, file notes etc) to evidence the review and subsequent decision.

7.7.8 Record-Keeping of Financial Promotions

The Firm will keep records of financial promotions it makes and/or approves for at least 5 years.

With reference to unregulated collective investment schemes, financial promotions records must include evidence that proves reasonable care has been taken to ensure the financial promotion has only been made to those entitled to receive it. The Firm and ARs must maintains records relating to potential investors/classes of potential investors targeted, together with supporting evidence relevant to their eligibility under the exemptions.

7.8 Client Agreements

The Firm and ARs are obliged to provide its clients with certain details about the Firm/AR (COBS 2.2A.1 R) and is required to put in place a written agreement between the client and the Firm/AR (COBS 8A.1.4 UK (a) and (c)) before services are provided, or before a client is bound by any proposed agreement. This agreement may be in the form of an engagement letter.

The Firm's policy is to keep a record of the agreement for at least 5 years following the end of the relationship with the client.

Written agreements are expected to include, as a minimum:

- As set out in COBS 6.1ZA, information about:
  - The Firm.
  - Its services, including, where relevant, the nature and extent of investment advice being provided.
  - Information on communications, conflicts of interest and regulatory status including relevant restrictions (e.g. client types).
- The types of financial instruments and nature of financial transactions that might be contemplated.
- Where relevant, details of safeguarding of client financial instruments or client funds.
- A clear description of costs and associated charges.

7.9 Disclosure of Side Letters with Material Terms

The Firm will not normally operate side letters, but if this occurred on an exception and justifiable basis, the Firm will disclose the existence of any side letters which contain any 'material terms' that it is aware of. The Firm defines a material term using the Alternative Investment Management Association's definition as follows:

'Any term the effect of which might reasonably be expected to be to provide an investor with more favourable treatment than other holders of the same class of share or interest which enhances that investor's ability either (i) to redeem shares or interests of that class or (ii) to make a determination as to whether to redeem shares or interests of that class, and which in either case might, therefore, reasonably be expected to put other holders of shares or interests of that class who are in the same position at a material disadvantage in connection with the exercise of their redemption rights.'

The disclosure of any side letters in existence will be made on a periodic basis in an appropriate medium including any formal external reports and in line with the industry guidance. Additionally, disclosure will be made to any potential new investors prior to their investing.

8a CONDUCT OF BUSINESS (COBS) – ADVISORY

This chapter covers COBS issues for advised and non-advised services (i.e. arranged/execution) only.

8a.1 Suitability of Investment Advice

COBS 9A.2.1 R requires the Firm and its ARs where they are providing recommendations to ensure the advice provided is suitable for the client's circumstances, investment objectives and attitude to investment risk.

The Firm and its ARs are permitted to provide investment advice to, and arrange investments for, Professional Clients (investment advice is not Eligible Counterparty business). Where the Firm/AR provides an investment service to a **Per Se** Professional Client it shall be entitled to assume that in relation to the products, transactions and services for which it is so classified, the client has the necessary level of experience and knowledge for the purposes of point (c) of COBS 9A.2.4 UK.

Where that investment service comprises the provision of investment advice to a **Per Se** Professional Client, the Firm/AR shall be entitled to assume for the purposes of point (b) of COBS 9A.2.4 UK that the client is able financially to bear any related investment risks consistent with the investment objectives of that client.

These assumptions would normally be detailed in relevant agreements.

At the point a client is first taken on and its client category is determined as an **Elective** Professional Client, the client's knowledge and experience is assessed in the context of the service and/or financial instruments then contemplated. For MiFID business, as per COBS 3.5.3 R the quantitative test must also be satisfied.

ARs must provide a completed Elective Professional Client notice and relevant KYC documents to the Firm for review and approval prior to the AR agreeing services with the AR's new client. Only once approval from the Firm has been received can the AR be sent terms and conditions for signing.

This status must be regularly reviewed and, in particular, before providing advice, the Firm/AR must ensure that the service and/or financial instrument currently being contemplated does not fall outside that originally contemplated (in relation to which the client's knowledge and experience was assessed).

If the client does not possess sufficient knowledge and experience then the Firm/AR cannot continue to categorise that client as an Elective Professional Client for the new contemplated service and/or financial instrument. However, the Firm/AR may continue to categorise them as Elective Professional Clients for the original service and/or financial instruments.

8a.2 Appropriateness for Non-Advised Services

COBS 10A.2.1R requires the Firm/AR to obtain from its client, information regarding that client's knowledge and experience in the investment field relevant to the specific type of product or service offered or demanded to enable the Firm/AR to assess whether the service or product envisaged is appropriate for the client.

As set out in COBS 10A.2.4 UK, when assessing a client's knowledge and experience, the Firm/AR will ensure the information it considers from the client includes the following to the extent appropriate to the nature of the client, the nature and extent of the service to be provided and the type of product or transaction envisaged, including their complexity and the risks involved:

- The types of service, transaction and financial instrument with which the client is familiar.

- The nature, volume, and frequency of the client's transactions in financial instruments and the period over which they have been carried out.
- The level of education, and profession or relevant former profession of the client or potential client.

The Firm/AR must not discourage the provision of information by a client/potential client for the purpose of assessing their knowledge and experience.

The Firm/AR is permitted to rely on relevant information provided by its client unless it has reason to be believe it is manifestly out of date, inaccurate or incomplete. The Firm/AR may also use information it already has in its possession, subject to compliance with appropriate data protection requirements.

Depending on the circumstances, the Firm/AR may be satisfied that the client's knowledge alone is sufficient for them to understand the risks involved in a product or service. Where reasonable, the Firm/AR may infer knowledge from experience.

Subject to applicable data protection rights, the Firm/AR is under no duty to communicate its assessment to the client.

If the Firm/AR assesses the client as having insufficient knowledge and experience for the product or service, it cannot provide the product or service to which the assessment relates.

As under section 8.1 above, the Firm/AR shall be entitled to assume that a Per Se Professional Client has the necessary experience and knowledge in order to understand the risks involved in relation to those particular investment services or transactions, or types of transaction or product, for which the client is classified as a Per Se Professional Client.

8a.3 Record-Keeping

The Firm and its ARs are required to keep orderly records of its business and internal organisation, including all appropriateness/suitability assessment, services provided and transactions arranged, for at least 5 years from the date the relationship ended or the conclusion of the transaction.

8b CONDUCT OF BUSINESS (COBS) – MANAGEMENT

This chapter covers investment management COBS issues for the Firm only.

IMPORTANT: ARs are not permitted to conduct investment management activity or act with discretion in respect of investment decisions.

8b.1 Suitability Management Decisions

COBS 9A.2.1 R requires the Firm, where it makes a decision to invest/trade, to ensure the decision made is suitable for the client's circumstances, investment objectives and attitude to investment risk.

The Firm is authorised to manage investments for Professional Clients (investment management is not Eligible Counterparty business). The client must be categorised as either a **Per Se** Professional Client or an **Elective** Professional Client in line with COBS 3.5. Where the Firm provides an investment service to a **Per Se** Professional Client it shall be entitled to assume that in relation to the products, transactions and services for which it is so classified, the client has the necessary level of experience and knowledge for the purposes of point (c) of COBS 9A.2.4 UK.

These assumptions would normally be detailed in relevant agreements.

At the point a client is first taken on and its client category is determined as an **Elective** Professional Client, the client's knowledge and experience is assessed in the context of the service and/or financial instruments then contemplated. For MiFID business, as per COBS 3.5.3 R the quantitative test must also be satisfied. This status must be regularly reviewed and in particular before providing advice the Firm must ensure that the service and/or financial instrument currently being contemplated does not fall outside that originally contemplated (in relation to which the client's knowledge and experience was assessed).

If the client does not possess sufficient knowledge and experience then the Firm cannot continue to categorise that client as an **Elective** Professional Client for the new contemplated service and/or financial instrument – the Firm may continue to categorise them as **Elective** Professional Clients for the original service and/or financial instruments.

The Firm's clients include funds it manages and those funds' investors. Funds will normally qualify as **Per Se** Professional Clients. A fund's investors will need to be assessed and confirm via the Professional Client notice whether it is a **Per Se** or **Elective** Professional Client before investing.

8b.2 Best Execution

The Firm is required to provide best execution, COBS 11.2. The Firm is not obliged to provide best execution when dealing with Eligible Counterparties (COBS 1 Annex 1 Application) but is obliged to when executing or transmitting orders on behalf of Professional Clients.

COBS 11.2A.2 R obliges the Firm to ensure all reasonable steps are taken to obtain, when executing orders, the best possible result, i.e. the terms are those most favourable to its client.

COBS 11.2A.20 R requires the Firm to have in place an order execution policy (OEP) that delivers terms that are most favourable to its client. The Firm's OEP is retained as a standalone policy document, separate to this Manual – Appendix E.

8b.2.1 Client Order Handling

COBS 11.3 does not apply to Eligible Counterparties (COBS 1 Annex 1 Application), but it does apply to Professional Clients. Since the Firm does not always execute orders (the broker does this as the client's agent), COBS 11.3 does not apply to the Firm in these circumstances, and these obligations lie with the broker COBS 11.3.13 G (2) and (3). The Firm is obliged to ensure orders are passed to brokers promptly and accurately recorded and allocated where applicable (COBS 11.3.2A UK). Further detail on client order handling is contained within the OEP.

8b.2.2 Record-Keeping – Client Orders and Transactions

Article 74 of the MiFID Org Regulation states: An investment firm shall, in relation to every initial order received from a client and in relation to every initial decision to deal taken, immediately record and keep at the disposal of the FCA at least the details set out in Section 1 of Annex IV to the Regulation (reproduced at COBS 11.5A.4 UK) to the extent they are applicable to the order or decision to deal in question.

Article 75 of the MiFID Org Regulation states: 'An investment firm shall, immediately after receiving a client order or making a decision to deal to the extent they are applicable to the order or decision to deal in question, record and keep at the disposal of the FCA at least the details set out in Section 2 of Annex IV' (reproduced at COBS 11.5A.5 UK).

8b.3 Personal Account Dealing (PAD)

COBS 11.7A.5 UK obliges the Firm to have in place and to maintain adequate arrangements relating to personal account dealing, aimed at preventing conflicts of interest, market abuse and inappropriate disclosure of otherwise confidential information about clients by partners and other members of staff. These arrangements are captured in section 3 and 4 of this Manual and in Appendices D, F, H and J.

8b.4 Valuation of Complex Illiquid Instruments

The Firm understands that it is important that investment managers are not able to influence the valuations of any funds that they manage. Any funds are valued by a third party, i.e. the fund(s') administrators. Additionally, it is important that the activities of the administrator are aligned with those of the Firm and that both parties understand the role and importance of the other. Reconciliations between the parties are carried out regularly.

8b.5 Reporting to Clients

8b.5.1 Introduction

COBS 16A requires the Firm to provide clients with certain occasional and periodic information.

COBS 16, relating to non-MiFID provisions, does not apply to Eligible Counterparties (COBS 1 Annex 1 Application).

8b.5.2 Periodic Reporting

When managing investments, clients must be provided with a periodic statement.

COBS 16A.4 requires the Firm, as an investment manager (performing portfolio management), to provide periodic reports to Professional Clients. COBS 16A.4.1 UK requires the Firm to supply to its investment management clients details of executed transactions (i.e. contract notes) if the client so requests.

COBS 16.3.10R specifies that in relation to non-MiFID business the Firm does not need to provide periodic statements to a client habitually resident outside the UK if the client has so requested or the Firm has taken reasonable steps to establish that the client does not wish to receive it.

The Firm must retain a record of periodic statements for 3 years from the date of despatch.

8b.5.3 Occasional Reporting

The Firm provides investment management services only therefore the COBS rules relating to occasional reporting do not apply (COBS 16A.3).

8b.5.4 Statements of Client Financial Instruments or Client Funds

The Firm is not authorised to hold or administer client assets or money. The Firm is not, therefore, required to comply with the provisions of COBS 16A.5.

8b.6 Stewardship Code

The Firm is required to disclose whether it has signed up to and follows the Stewardship Code on Corporate Governance for institutional investors or if it does not follow the Code, to explain its alternative arrangements. This information is disclosed on the Firm's website.

8b.7 Shareholder Rights Directive (SRD II)

The first SRD, SRD I, came into force in 2007 and was implemented in the UK through amendments to the Companies Act 2006. SRD II made amendments to SRD I and came into force in 2017. As before, the UK implemented relevant aspects of SRD II through amendments to the Companies Act 2006 but also through the passing of a number of new statutory instruments, such as the Shareholder Rights Directive (Asset Managers and Insurers) Instrument 2019, which amended parts of SYSC 3 and 10 and COBS 2 for relevant firms. SRD II requires asset owners (institutional investors) and asset managers to make disclosures about their long-term investment strategies, their arrangements with each other and their engagement with the companies they invest in. The rules seek to improve transparency by enhancing the flow of information across the institutional investment community, and by promoting common stewardship objectives between institutional investors and asset managers.

The Directive also recognises that certain persons (related parties) may have an influence on companies they invest in, and that the nature of transactions with related parties (RPTs) may affect shareholders' assessment of company valuation. The requirements build on the accounting framework set under International Financial Reporting Standards. SRD II requires companies with shares admitted to trading on regulated markets to disclose and have other safeguards in place for material transactions with related parties.

Some of the key SRD II requirements listed in COBS 2.2B and DTR 7.3.8R include requiring firms to:

- Publicly disclose their shareholder engagement policies, and annually publish how they have implemented such policies.
- Disclose to asset owners the manager's shareholder engagement activities.

Disclose related party transactions at the latest at the time of the transaction (For UK companies with shares admitted on a regulated market).

The transparency requirements applying to asset managers, includes MiFID investment firms, AIFMs (excluding small AIFMs), UCITS management companies, self-managed UCITS funds and FCA-regulated insurers. Whilst this may not cover the full universe of institutional investor, the SRD II changes should be considered alongside the Financial Reporting Council's revisions to its Stewardship Code.

9 PRODUCT OVERSIGHT AND GOVERNANCE

9.1 Introduction

This section of the Manual sets out the Firm's approach to the FCA's product oversight and governance regime, the rules of which are set out in the PROD sourcebook. Appendix Q can be found in the Manual Appendices, and provides an assessment questionnaire for the Firm to complete in respect of each new and existing product and service as to their current compliance with the PROD rules, and thus an indication of further action that may be required. The PROD assessment should be completed when any new product or service is launched and also on an ad hoc basis (fund closes etc). Although much of the focus is on products, the rules also capture services and should be applied accordingly.

9.2 Background

The FCA's product oversight and governance rules came into force on 3 January 2018 in line with the introduction of MiFID II. Although the FCA had product governance requirements before the introduction of MiFID II, these were narrower in scope than the new rules in terms of the financial instruments they covered.

In simple terms, the product governance element of MiFID II is aimed at ensuring advisers are offering their clients suitable solutions, by requiring product manufacturers and distributors, such as advisers, to identify target markets. It is therefore vital that firms to which the PROD rules apply ensure they have structured their business approach accordingly and are able to demonstrate the application of these rules.

9.3 The Product Oversight and Governance Regime

9.3.1 Definitions

Product oversight and governance means the systems and controls firms have in place for the design, approval, marketing and ongoing management of products and services throughout their lifecycle, to ensure they meet legal and regulatory requirements. If these systems and controls are working effectively then products will:

- Meet the needs of one or more identifiable target markets.
- Be sold to clients in the target markets by appropriate distribution channels.
- Deliver appropriate client outcomes.

The FCA define a manufacturer as a person creating, developing, issuing and/or designing an investment, including when advising corporate issuers on the launch of new investments.

The definition of a distributor is a person offering, recommending, or selling an investment, or providing an investment service to a client.

9.3.2 PROD Sourcebook

The FCA's PROD sourcebook is split into 4 sections, but only the first 3 apply to the Firm and its ARs:

- PROD 1. Product intervention and product governance sourcebook, providing a summary of each of the 4 PROD sections.

- PROD 2. Statement of policy with regards to making of temporary product intervention rules, is the FCA's position on when it will intervene with regards to a product and apply temporary restrictions.
- PROD 3. Product governance: MiFID, sets out the rules to be applied for both the manufacture and distribution of a product that falls under the MiFID umbrella.
- PROD 4. Product governance for insurance-based investment (IDD) products.

In summary, PROD 1 and 2 provide information, whilst PROD 3 sets out action to be taken. This Manual only considers PROD 3 requirements as the Firm does not have the regulatory permissions to conduct insurance-related business. PROD 3 thus applies to MiFID investment firms, CRD credit institutions, MiFID optional investment firms, and branches of third-country investment firms. For non-MiFID firms that manufacture or distribute financial instruments, the FCA has stated that these firms should (as opposed to must) follow the PROD rules. Therefore, the Firm has opted to apply the principles of the PROD regime to non-MiFID business which includes acting as an AIFM.

As a principal, the Firm has the responsibility to oversee the regulated activities of its ARs, and ensure these activities fall with the perimeter of its authorised permissions. This then means that any AR which manufactures, and/or distributes a financial instrument must comply with the PROD 3 sourcebook.

For manufacturers and distributors in scope of PROD 3, there are several overarching key elements that must be complied with, as follows:

9.3.3 Manufacturers

For manufacturers of financial instruments:

- The product is designed to meet the needs of the client target market (i.e. Professional Clients and/or Eligible Counterparties' business clients).
- That the strategy for the distribution of the product is compatible with this target market.
- That the product is actually distributed to the target market.
- That where new products have been developed or existing products are being significantly modified, a process of approval has been followed.
- That risks associated with the design of the product and its intended target market have been assessed and mitigated.
- That where products have been manufactured in collaboration with other firms, a written agreement outlining mutual responsibilities must be in place.
- That products undergo scenario testing and analysis to assess the risks of poor outcomes for clients and the circumstances in which those poor outcomes arise.
- That sufficient information is available to intended and existing distributors of new and existing products covering the functioning of the product, the approval process, the target market, and appropriate distribution channels.
- That the product manufacturer has a robust review process is in place to ensure the product remains fit for the purpose of its intended target market.
- That the product manufacturer has considered and reviews potential and actual conflicts of interest to ensure no client is adversely impacted and market integrity issues are not created.
- That sufficient oversight and training mechanisms are in place to enable sufficient governance of the manufacturing process and the knowledge of personnel involved in this.
- That monthly compliance reports include details of the products manufactured and the distribution strategy.

9.3.4 Distributors

For distributors of financial instruments:

- That a comprehensive understanding and knowledge of the product being provided is obtained via information provided by the manufacturer.
- That the target market is clearly identified, even if not specified by the manufacturer, and this aligns with the target market of the distributor.
- That a distribution strategy is set out, considering wider FCA rules, as necessary.
- That appropriate governance arrangements are in place.
- That personnel involved in the distribution of the product have the necessary knowledge and understanding of the product to do so effectively.
- That compliance reports include details of the products distributed by the firm.
- That a robust review process is in place to ensure the product remains fit for the purpose of its intended target market, and its governance arrangements provide sufficient oversight.
- That a process is in place to provide feedback to the manufacturer on sales and reviews undertaken.
- That where the distribution of a product is to another distributor, the responsibilities in this chain are understood. Where this applies, please refer to section 9.5 below, which contains the policy and procedure for the appointment of introducers and placement agents.

9.4 PROD Annex Assessment Questionnaire

9.4.1 Assessment Questionnaire

The Firm will provide each new AR with a blank PROD assessment questionnaire to complete once the AR entity has been appointed by the FCA. Once the AR has completed the PROD assessment, the Firm will review it to establish the AR's current level of compliance with the rules and whether the AR is conducting its regulated activity as a manufacturer and/or a distributor. The Firm's review will be recorded in the Firm's version of the assessment questionnaire in Appendix Q. ARs should complete the required sections of the assessment themselves, as this will be picked up as part of monitoring, and report changes to the Firm. Existing ARs will be required to update and/or complete a new PROD assessment on an ad hoc basis also (launch of new product/fund, fund closes etc).

9.4.2 Follow-Up

If on completion of the assessment questionnaire there are identified compliance gaps, the AR must report these to the Firm and take the necessary action to address the issues at hand. There is no defined solution as it is dependent on the context of each AR firm. However, actions may require, but are not limited to:

- Putting in place policies.
- Training staff.
- Defining a process.
- Identifying the product target market.
- Identifying conflicts of interest.
- Establishing appropriate management information.
- Establishing a monitoring regime.
- Establishing a product review mechanism.
- Establishing a feedback loop.

Sign-off for implemented actions to address any gaps will be undertaken by the Compliance Officer or a member of the compliance team, delegated from the Compliance Officer.

9.5 Third-Party Placement Agents/Introducers

9.5.1 General Requirements

As set out in section 3.15 of the Manual, outsourcing should not:

1. Create additional operational risk.
2. Jeopardise internal controls.
3. Delegate responsibility or change client relationships.
4. Hinder the FCA/internal compliance monitoring.
5. Prevent continued compliance with the Firm's threshold conditions or Principles for Businesses.

The Firm/AR and its senior management remain fully responsible for discharging all of its obligations under the regulatory system in relation to any outsourced function. In other words, the activity can be outsourced but not the responsibility.

The Firm/AR must make sure that any service provider:

- Is competent and capable to carry out the activity.
- Has the necessary authorisation(s)/licence(s) or arrangement(s) to enable the activity to be carried out lawfully.
- Signs a valid, written agreement with the Firm/AR that clearly allocates and sets out rights and responsibilities, and which ensures effective performance against agreed standards, e.g. service level agreement, regular review and monitoring, escalations, service credits etc.

SYSC 8.1.8 R contains necessary steps for certain regulated firms to take when outsourcing critical or important operational functions. However, these are considered as good practice guidance for other firms and in relation to other types of outsourced activity and should be considered prior to the appointment of every third-party service provider. The remainder of this policy relates to the systems and controls regarding third-party placement agents and/or introducers.

9.5.2 Placement Agents and Introducers

Placement agents typically assist fund managers with fundraising by helping structure the transaction and/or find potential investors that are willing and able to invest in offered securities. The agent acts on behalf of the fund manager and does not purchase the offered securities directly.

Introducers have a much more limited scope of appointment than placement agents and their activities tend to be limited to effecting introductions to the fund manager or other members of the fund group and distributing approved communications on behalf of the fund manager.

Both types of firm/individual work on behalf of the fund manager, therefore, these firms/individuals must not provide any advice on the transactions/offerings to which their activities relate, and the fund manager is ultimately responsible for the activities of these firms/individuals and must, therefore, be involved in the appointment process including the putting in place of an appropriate agreement.

The activities of placement agents and introducers are likely to fall within scope of the regulated activities of arranging investments and making arrangements with a view to transactions in investments. Therefore, placement agents and introducers will need to have the necessary authorisation, licence or arrangement in place to enable them to conduct this activity lawfully. Where a placement agent or introducer has no authorisation, licence or arrangement, this should be investigated under the direction of the Firm's

Compliance Officer. It's important to note that the 'all crimes' approach of POCA means that any advantage gained through unlawful activity would constitute proceeds of crime.

Legislation relevant to the fund and/or fund manager will also impose restrictions and limitations on the activities of placement agents and introducers. For example, UK AIFs can only be marketed, directly and indirectly, outside the UK in accordance with local rules and regulations, such as the third-country rules under National Private Placement Regimes in EU member states.

Therefore, as well as general outsourcing risks, the use of placement agents and introducers creates additional compliance and legal risks for the fund manager and connected parties.

9.5.3 Procedure for Appointing Placement Agents and Introducers

When the Firm/AR is considering appointing a placement agent or introducer, it must first notify the Firm's Compliance Officer of the proposed scope of appointment and provide an updated PROD assessment that takes into account the proposed appointment. Any directions given by the Compliance Officer must be followed.

General outsourcing requirements, as set out above and in section 3.15 of the Compliance Manual, and the following steps specific to the appointment of a placement agent/introducer, must then be followed by the Firm/AR:

1. Notify the Compliance Officer of the names of the firms/individuals it wishes to appoint and provide the Compliance Officer with the due diligence conducted on the proposed appointments, which demonstrate the proposed appointments are considered to be suitable in respect of the general outsourcing requirements.
2. The Compliance Officer will review the information provided and may conduct or request further due diligence be carried out.
3. The Compliance Officer will then confirm whether or not the proposed appointments are appropriate. If they are, the Firm/AR should provide the Compliance Officer with the proposed agreement so that the agreement can be checked for appropriateness, required terms and conditions.
4. Where an AR is permitted to appoint a placement agent or introducer, the AR must ensure:
    a. The Firm is kept informed of all activities and involved in all decisions relating to the placement agent/introducer including approval of target recipients.
    b. It holds regular (at least monthly), documented performance reviews/evaluations of the placement agent or introducer with respect to the terms of appointment, as set out in the relevant agreement.
    c. Reports to the Firm on the activities and performance of all placement agents/introducers in the relevant sections of the monthly report templates.
    d. Informs the Firm, without delay, of any issues or concerns regarding a placement agent or introducer.

When an AR is considering terminating or not renewing an agreement with a placement agent or introducer, it must do so in full compliance with the terms of the agreement and must notify the Firm of its intentions in advance and without delay, separately and in addition to monthly reporting.

10 CLIENT ASSETS

10.1 Introduction

The Firm is permitted to control but not hold client money. If it (or any of its ARs) held client money, i.e. client money was paid into a named account of the Firm or its ARs, then this would be a breach of the Firm's scope of permission. In addition, CASS 7 rules apply to holding client money and therefore it is likely that the Firm would also be in breach of these rules.

Although the Firm's permission allows it to control client money, i.e. carry out activities on client money that is in a named account of the client, in practice it does not normally do this for clients. Where it is deemed to be doing so, in line with 10.3 below, it will comply with the 'mandate' rules at CASS 8 including having a list of authorised signatories for any particular client and taking appropriate security measures on any payment instruments.

As a Firm with AIFM permission, technically this permission does permit the Firm to 'hold' client assets where its management activities come under AIFMD. However, it does not have this permission for MiFID management activities. Holding such assets normally means being appointed as custodian and responsible for both safeguarding and administration of assets. However, in practice, the Firm does not carry out this activity on behalf of any fund clients.

Client assets are deemed to be legal titles to any designated investments, i.e. for securities, either physical share certificates or dematerialised (i.e. electronic) securities. If the Firm is deemed to be holding, i.e. acting as custodian for client assets rather than the appointed custodian or administrator of a fund, CASS 6 rules may apply including the safekeeping and recording of any assets.

In the event that either the Firm or its ARs receive such assets on a temporary basis, these should either be forwarded to the relevant client as soon as possible, normally within 24 hours, where this is a 'third-party' client. Or where the client is an associated entity, this must be clearly allocated to a client's files (either online or physical) within the same timescales. Whilst doing so, in line with FCA Principle 10, these assets should be kept securely, and a record maintained.

For any firms that are deemed to be acting both as custodian and carrying out 'administration' on these client assets, CASS 6 rules in the CASS sourcebook will be directly applicable to that firm.

Otherwise, the Firm is permitted to arrange for the custody and control of client assets, i.e. appoint a custodian, but not hold the client assets, in which case the procedure below must be followed.

10.2 Procedure

It is important to note again at this stage that ARs are not permitted to conduct investment management activity or act with discretion in respect of investment decisions.

Each fund shall appoint an administrator who will be responsible for calculating the net asset value (NAV) and where relevant, a separate custodian may be appointed who will be responsible for custody of the assets/money.

In practice, the fund administrator will normally take responsibility for the reconciliation of investors' funds including the calculation of NAV. The majority of investment management decisions are taking place in unlisted securities or loans which are therefore not taking place on trading markets. However, in the unlikely position that trades in listed securities take place, the following procedure would also apply.

1. The investment manager must have a record of all trading orders in the 'trading book' at the time of placing orders on a trading market or immediately after.
2. Where relevant, and an order is placed on a trading market, at the end of a trading day a trade file including all executed orders in the day must be sent to the administrator and custodian by the investment team. In practice, this will be carried out by the AR as investment adviser to (not manager of) the fund client.
3. If relevant, where a trade is placed on a trading market, on the following day the team must obtain and reconcile any broker confirmations to the trade file. Any dealing errors/abnormalities must be brought to the attention of the relevant investment manager immediately who will record any such dealing errors in the dealing error register and address the error to ensure that the client has not been disadvantaged in any manner. All discrepancies are investigated.
4. At the end of any relevant period, the investment manager (or investment adviser where the fund is a client of the AR) will reconcile all cash and investment positions with the administrator before the administrator releases the NAV.

10.3 Mandate Authorities

If the Firm or its ARs are deemed to be controlling client money under CASS 8, the investment manager will maintain an up-to-date list of the authorities granted to the Firm by its clients and any restrictions that apply – whether internally or externally imposed.

Records will be kept of all transactions entered into, and of the internal controls that are in place to ensure that these transactions are within the scope of the authority granted to us. Any documents belonging to the clients should normally only be held by the administrator. In the unlikely event that the investment manager holds client documents on a temporary basis, these will be held and transferred securely as soon as possible.

11 TRAINING AND COMPETENCE

11.1 The Firm's Commitment

In accordance with Principles 2 and 3, SYSC 5, and in order to mitigate elements of its conduct risk profile, the Firm commits to ensure:

- Its staff and individuals within its ARs are competent.
- Its staff and individuals within its ARs remain competent for the work they do.
- Its staff and individuals within its ARs are appropriately supervised.
- The competence of its staff and individuals within its ARs is regularly reviewed.
- The level of competence is appropriate to the nature of the business being conducted.

11.2 General Requirements

SYSC 5 outlines that a firm must employ personnel with the skills, knowledge and expertise necessary for them to properly discharge the responsibilities allocated to them. A firm's systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it. This includes assessing an individual's honesty and competence.

As a common platform firm, the MiFID Organisational Regulation and the following FCA specific rules/guidance, as set out in SYSC 5.1, apply to the Firm:

- Competent employees rule:
    - A firm's systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it. This includes assessing an individual's honesty and competence. This assessment should normally be made at the point of recruitment. An individual's honesty need not normally be revisited unless something happens to make a fresh look appropriate.
    - Any assessment of an individual's suitability should take into account the level of responsibility that the individual will assume within the firm. The nature of this assessment will generally differ depending upon whether it takes place at the start of the individual's recruitment, at the end of the probationary period (if there is one) or subsequently.
- Knowledge and competence:
    - A firm must ensure, and be able to demonstrate to the FCA, at the FCA's request, that any relevant individuals possess the necessary knowledge and competence so as to ensure that the firm is able to meet its obligations under the relevant COBS and PROD rules.
    - ESMA has issued Guidelines specifying the criteria for assessment of knowledge and competency and firms are expected to act consistently with the guidelines.
    - Appendices M and N contain a knowledge and competence assessment sheet and corresponding guidance, respectively. The Firm and its ARs use this sheet in order to initially assess relevant staff members and also as part of an annual assessment of relevant staff members.
- Segregation of functions:
    - A firm's senior personnel must define arrangements concerning the segregation of duties within the firm and the prevention of conflicts of interest.
    - The effective segregation of duties is an important element in the internal controls of a firm in the prudential context. In particular, it helps to ensure that not one individual is completely free to commit a firm's assets or incur liabilities on its behalf.

- Segregation can also help to ensure that a firm's Governing Body receives objective and accurate information on financial performance, the risks faced by the firm and the adequacy of its systems.
- In addition, appropriate segregation of duties (along with effective oversight) helps mitigate internal fraud risk.

11.3 Knowledge and Competence

To be assessed as competent, individuals providing investment advice and/or information must have achieved an appropriate qualification that meets ESMA's knowledge and competency guidelines and have at least 6 months' relevant full-time experience.

Candidates must meet knowledge and competency requirements within 48 months of starting and up to that point, must be supervised by an individual that, as a minimum, meets the requirements to act as a competent supervisor.

When assessing competence, initially and periodically thereafter, of all SMF and CF holders (at Firm level), Approved Persons at AR level, not just those holding CF30, should use the form in Appendix M, at onboarding and annually.

T&C records should demonstrate supervision of an individual is commensurate with the Firm's/AR's assessment of the competency of the individual, including their knowledge and experience. The rules permit outsourcing of supervision but highlight that the Firm/AR remains ultimately responsible for compliance with the requirements.

11.4 Attaining and Assessing Competence for Investment Advisers

No member of staff will be permitted to provide investment advice unless they have been assessed as competent to undertake these activities or engage in the activities whilst under appropriate supervision – the Firm/AR must be able to clearly demonstrate that supervision is appropriate.

AR CF30 supervision must be undertaken by an individual who is either CF30 approved and/or an individual certified for client dealing under the SM&CR. Kevin Gallacher is certified for client dealing and therefore will act as supervisor for any other client dealing certified staff or CF30s.

The Firm is not covered by the formal requirements of TC 2.1 in relation to assessing competence formally, as it cannot carry on retail investment activities but aims to comply with the spirit of rules under TC and, as set out above, must fully comply with the requirements in SYSC 5.1 and the ESMA guidelines for the assessment of knowledge and competence.

The Firm will not assess an investment adviser as competent to engage in or oversee the activity unless the individual is considered competent to apply the knowledge and skills necessary to engage in or oversee the activity without supervision.

The Compliance Officer maintains a written record of how an individual for the Firm or an AR was assessed as competent including the criteria applied and when the competence decision was arrived at. ARs must ensure they provide the Compliance Officer with sufficient records to demonstrate knowledge and competence requirements have been achieved within the required timeframe (48 months) and are being maintained.

11.5 Attaining and Assessing Competence for Investment Managers

This applies to the Firm only.

No member of staff will be permitted to act in the capacity of an investment manager unless they have been assessed as competent to undertake these activities or engage in the activities whilst under appropriate supervision – the Firm must be able to clearly demonstrate that supervision is appropriate.

Supervision must be undertaken by an individual who is certified for client dealing which includes investment advice and investment management. As such, Kevin Gallacher holds this Certified role at the Firm.

The Firm is not covered by the formal requirements of TC 2.1 in relation to assessing competence formally, as it cannot carry on retail investment activities but aims to comply with the spirit of rules under TC and, as set out above, must fully comply with the requirements in SYSC 5.1 and the ESMA guidelines for the assessment of knowledge and competence.

The Firm will not assess an investment manager as competent to engage in or oversee the activity unless the individual is considered competent to apply the knowledge and skills necessary to engage in or oversee the activity without supervision.

The Compliance Officer maintains a written record of how an individual for the Firm was assessed as competent including the criteria applied and when the competence decision was arrived at.

11.6 Ongoing Competence and Annual Review

By way of the routine AR monitoring process, the Firm's compliance team will review the TC records for each Approved Person and relevant individual (providing investment information).

MiFID II requires the Firm and its ARs to undertake annual reviews of competence, development needs and experience in accordance with the ESMA guidelines using the forms and guidance in Appendices M and N. Completed forms and relevant supporting documentation for each Approved Person and relevant individual must be provided to the Compliance Officer on request, who will review and approve the sign-off of each individual and/or give directions on action that needs to be taken to achieve or maintain competency. The Compliance Officer will also act as the 'assessor' for nominated senior managers of ARs. ARs must comply with any directions provided by the Compliance Officer fully in the time permitted.

The form in Appendix M is based on the relevant ESMA guidelines and, inter alia, takes into account:

- The individual's technical knowledge and skills, together with the day-to-day application of these in their role.
- Changes in the market, products, legislation, regulation etc relevant to their role and how they have kept up to date.
- Any training or development needs identified.

11.7 Failure to Obtain or Maintain Competence

Individuals that have not achieved competence within 48 months will not be permitted to continue in the role even with supervision. Therefore, training and development should be structured in such a way that the Firm/AR will be able to identify those that are unlikely to achieve competence within 48 months. Where this is identified the Firm or the AR must invoke the relevant HR/capability procedures and also inform the Firm's Compliance Officer.

The Firm and ARs should undertake regular monitoring of individuals. Where monitoring indicates competence issues, the Firm and relevant AR should investigate and implement appropriate supervision and an action plan to address the issue(s) promptly. The Firm's Compliance Officer should be informed about all competency issues without delay.

11.8 Training and Competence Records

The Firm and its ARs must retain the records (as noted above) for a period of at least 5 years after resignation of the individual from the Firm/AR. These records include both the initial competence assessment and the ongoing review of how individuals have remained competent.

In the event of an individual performing Controlled Function CF30 (or a Certification Function) under supervision, full records of this will be kept by the individual responsible for the individual's supervision. Copies of these records should be passed to the Compliance Officer on request. These records should also be kept for at least 5 years from the individual's resignation/termination date.

12 COMPLAINTS AND REDRESS

12.1 FCA Dispute Resolution (DISP): Complaints Sourcebook

The FCA DISP sourcebook sets out the rules on the handling of complaints, principally focused on eligible complainants (see 12.3 below). DISP provides for the establishment of an independent alternative (to the courts) dispute resolution scheme, the Financial Ombudsman Service (FOS), once the Firm's own complaints procedures have been exhausted.

Handling requirement rules are set out in DISP 1.1A and apply solely to MiFID complaints about MiFID investment firms from Retail Clients, Professional Clients and (in relation to Eligible Counterparty business) Eligible Counterparties, all of whom may or may not also be eligible complainants.

Any complaints received should be referred to the Firm's Compliance Officer, Gillian Gallacher, without delay.

12.2 Low-Impact Issues

If a client or prospective client raises low-impact issues, which the Firm or its ARs have the ability to resolve to the client's satisfaction at the point they are raised, the Firm or AR may take appropriate action to resolve the issues without seeking prior approval/instruction from the Firm's Compliance Officer. Once resolved, details of the issues raised, the resolution and acceptance of the resolution by the client must be logged at AR level and notified to the Compliance Officer without unreasonable delay.

A summary communication setting out the issues and resolutions should also be sent to the client within 5 working days of the issues being raised, along with a copy of the Firm's complaints management policy and the complaints leaflet.

If the client raises further issues, before any additional action is taken the situation must be discussed with the Compliance Officer without delay and their instructions followed.

12.3 Definition of Eligible Complainant

In the context of regulated activities undertaken by the Firm and its ARs, the Firm is not able to deal with Retail Clients. A Retail Client is one that does not meet the MiFID definition of Professional Client. Retail Clients will therefore include 'natural persons' acting wholly or predominantly outside their trade, craft, business or profession, such as high net worth individuals or a director of a corporate client where the regulated activities are being conducted in a personal capacity.

Eligible complainants also include 'micro-enterprises', which are enterprises that employ fewer than 10 persons and have a turnover or annual balance sheet that does not exceed €2 million. In this definition, an enterprise means any person engaged in an economic activity, irrespective of legal form and includes in particular, self-employed persons and family businesses engaged in craft of other activities and partnerships, or associations regularly engaged in an economic activity.

In addition, the definition of eligible complainant includes:

- A charity which has an annual income of less than £6.5 million.
- A trustee of a trust which has a net asset value of less than £5 million.
- A small business, which is:

    - Not a micro-enterprise, has an annual turnover of less than £6.5m (or its equivalent in any other currency) and
    - Has less than 50 persons or
    - A balance sheet total of less than £5m (or its equivalent in any other currency).
- A guarantor, which is a natural or legal person but not a consumer, and has given a guarantee or security in respect of an obligation or liability of a person which was a micro-enterprise or small business as at the date that the guarantee or security was given.

DISP 2.7.6 also outlines the type of relationships between a complainant and a respondent that would determine whether the activities being complained about involved an eligible complainant or not.

DISP 2.7.9. R contains a number of exceptions where clients would not be considered eligible complainants. The exceptions include a complainant that was Professional Client or an Eligible Counterparty in relation to the Firm/AR and activity in question at the time of the act or omission by the Firm or AR, which is the subject of the complaint.

As such, it is considered unlikely that the Firm and its ARs will deal with such eligible complainants, but it is possible, especially following the extension of the FOS remit from 1 April 2019. Therefore, whether a client meets the definition of an eligible complainant should be examined on a case-by-case basis **at the outset**. Should a client fail to meet the MiFID Professional Client definition and falls within the definition of an eligible complainant, upfront disclosures regarding FOS rights and all the complaints-handling rules in DISP 1.1A, inter alia, will apply.

In the unlikely event that the Firm or its ARs deal with an eligible complainant, or if there is any doubt about the eligibility of a client, guidance should be sought immediately from the Firm's Compliance Officer regarding the procedures to be followed.

12.4 Definition of a MiFID Complaint

DISP1.1A.3 G defines a MiFID complaint as, amongst other things, a complaint about:

- The provision of investment services or ancillary services to a client by an investment firm.
- The activities permitted by Article 6(3) of the UCITS Directive when carried on by a collective portfolio management investment firm.
- The activities permitted by Article 6(4) of the AIFMD when carried on by a collective portfolio management investment firm.

In essence, a complaint is any expression of dissatisfaction from a client, or prospective client, about the provision of an investment or ancillary service or product.

12.5 Awareness

At the request of clients and prospective clients, or when acknowledging a complaint, the Firm and its ARs, when the AR is subject to instructions from the Firm's Compliance Officer, should provide clients with a copy of the Firm's complaints management policy and a tailored copy of the document titled 'Not happy? Here's what to do'.

The Firm and its ARs should ensure details of the complaints-handling process are always easily accessible, e.g. by displaying the details in contractual documents or on websites.

12.6 Complaints Handling

If anyone at the Firm, at one of its AR firms, or anyone at a former AR of the Firm receives a complaint, the following procedures must be followed:

1. Any complaint received, whether verbally or in writing, must be notified to the Compliance Officer without delay.
2. Clients must be able to complain free of charge.
3. The complaint must be acknowledged in writing within 5 working days of its receipt either by the Compliance Officer or, on the instruction of the Compliance Officer, by the AR. A copy of 'Not happy? Here's what to do.' and the Firm's complaints management policy must be provided alongside the complaint acknowledgement.
4. Any further correspondence received from the complainant by anyone other than the Compliance Officer must forward this correspondence to the Compliance Officer without delay.
5. Unless directly involved in the nature of the complaint matter itself, the Compliance Officer will fairly, consistently and promptly:
    a. Add the complaint to the complaints log and create a file on Dropbox for related correspondence/documentation.
    b. Inquire into the facts surrounding any complaint.
    c. Establish the complainant's demands.
    d. Gather and investigate all relevant evidence and information, including but not necessarily limited to emails, agreements, and testimony.
    e. Make reasonable effort to keep the complainant updated with the progress of their complaint.
    f. Attempt to resolve the complaint as quickly as possible, but in any case, issue a final decision within 4-8 weeks of its receipt.
    g. Within the response the following must be provided: a clear explanation of the Firm's position; its reasons for it taking this stance; where appropriate, the level of redress being offered and how this was calculated; and the options left to the complainant should they wish to maintain the complaint.
    h. When a response within expected time limits is not possible, the complainant should be informed about the reason(s) for the delay and provided with an indication of the expected timeframe in which the Firm will be able to respond.

The Compliance Officer will ensure that complaints are investigated competently, diligently and impartially. Additional information should be obtained as necessary.

The Compliance Officer will appoint a deputy (either a partner or compliance manager) to investigate any complaint where the Compliance Officer is the subject matter of the complaint.

When investigating complaints, the Compliance Officer will consider whether there are any signs of recurring or systemic problems. Where signs are identified the Compliance Officer will identify the steps the Firm or its AR need to take to remedy these.

The Compliance Officer will maintain a file of all complaints received, resolutions to complaints and any subsequent correspondence.

12.7 Record-Keeping

In accordance with DISP1.9, and on the legal basis of the Firm's legitimate interests in being able to defend against claims and respond to relevant requests for information from competent authorities, the Firm will

keep records of each complaint received (as set out above) for at least 5 years from the date the complaint was received.

These records will be kept by the Compliance Officer.

12.8 Complaints Reporting

The Compliance Officer will provide information on complaints and complaints handling to the FCA:

- In response to ad hoc requests from the FCA.
- As part of the Firm's regular reporting cycle through RegData – 6-monthly complaints return (DISP 1 Ann1R).
- Where required under SUP 15.

In addition, where required by applicable law or regulation, the Compliance Officer will also provide information relating to complaints and its handling of complaints to an alternative dispute resolution provider.

12.9 Complaints Oversight Officer

In accordance with DISP 1.3.7, Gillian Gallacher has been nominated as the Complaints Oversight Officer for the Firm and will have responsibility for oversight of the Firm's complaints handling.

12.10 Financial Services Compensation Scheme

As the Firm is not permitted to deal with Retail Clients, it is normally unlikely to deal directly with any eligible claimants under the Financial Services Compensation Scheme (FSCS) (as defined by FCA rules at COMP 4.2) or 'protected investment business claims' (as defined by COMP 5.5). FSCS costs are only in scope where income arises which is attributable to both an eligible claimant and a 'protected claim'.

Investment funds for which the Firm provides investment management activities on behalf of fund advisory ARs are not eligible claimants in their own right. Other non-fund advisory clients are unlikely to satisfy the definition of eligible claimant as these are normally of a size or nature excluded under COMP 4.2.2, and/or no eligible income (as defined by FEES 6) arises from these activities.

Although the Firm has ordinarily been exempt from annual contributions to the FSCS and its costs, rules introduced in April 2018 require the Firm to 'look through' funds under management and identify if any of the underlying investors would in themselves be eligible claimants if the fund falls under the scope of COMP 5.5.3. This includes authorised funds, but excludes non-UK domiciled funds, or funds that are a body corporate. If a fund remains in scope then FSCS costs in relation to any income attributable to eligible claimants will need to be calculated and where appropriate, passed onto the relevant ARs on an annual basis.

On an ongoing basis, the Compliance Officer will review this in relation to its clients, including ARs, on a case-by-case basis considering the above.

13 REPORTING AND NOTIFICATIONS

13.1 Annual Controller's Report

The Firm is required to keep the FCA informed about the identity of its controllers.

A controller's report must currently be submitted via RegData to the FCA annually, within 4 months of the Firm's accounting reference date (financial year end). The Firm's accounting reference date is 31 March, and therefore the deadline is 31 July each year.

The report must be in the format prescribed by the FCA and contain a list of all the controllers as at the Firm's accounting reference date of which the Firm is aware, and for each controller, may need to state:

- Their or the entity's name.
- The percentage of voting power in the Firm, or – should it become relevant – a parent company undertaking which it is entitled to exercise (or control the exercise of), whether alone or with any associate.
- The percentage of shares in the Firm, or if it becomes relevant a parent company undertaking which it controls/holds as above, whether alone or with any associate.
- If the controller is a body corporate, its country of incorporation, address and registered number.
- If the controller is an individual, their date and place of birth.

A current structure chart (as at period end date) should be included with each return. If applicable, a group organisation chart might be required.

If there have been no changes in the identity of the Firm's controllers or if the Firm is not aware of any changes in the percentages of shares or voting power in the Firm held by any controllers (alone or with any associate), then the latest controller's report should confirm this.

Notwithstanding this annual reporting requirement, any significant change in control during the year would require FCA notification and possibly prior FCA clearance (see below) under SUP 11.

13.2 Annual Close Links Report

Threshold Condition 3 (Close Links) advises that if the Firm has close links with another person, the FCA must be satisfied that:

- Those close links are not likely to prevent the FCA's effective supervision of the Firm.
- Where it appears to the FCA that the person is subject to the laws, regulations or administrative provisions of a territory which is not an EEA State, neither, the foreign provisions, nor any deficiency in their enforcement, would prevent the FCA's effective supervision of the Firm.

The Firm must submit a close links report, RegData, to the FCA annually, containing the information below, and in the format prescribed by the FCA. This must be submitted within 4 months of the Firm's accounting reference date. The deadline for submission is therefore 31 July each year.

If the Firm is not aware:

- Of any close links to the Firm or
- Of any material changes in respect of the Firm's close links since the submission of the previous report

then the report should also confirm this. An up-to-date structure chart (as at period end) showing close links should be included.

The report must contain a list of all persons with whom the Firm has close links as at the Firm's accounting reference date of which the Firm is aware, and for each such link state:

- Its name.
- The nature of the close link.
- If the close link is with a body corporate, its country of incorporation, address and registered number.
- If the close link is with an individual, their date and place of birth.

13.3 Annual Financial Crime Report

The Firm is required to submit the annual financial crime report under SUP 16.23. Firms need to provide this information to the FCA to ensure it receives information about the Firm's systems and controls in preventing financial crime.

The REP-CRIM is to be submitted via RegData to the FCA annually within 60 business days of the accounting reference date. As the Firm's accounting reference date is 31 March, the deadline is 23 June each year, beginning in 2023.

The report includes information on (amongst other things):

- Jurisdictions in which the Firm operates.
- PEPs and PEP relationships.
- High-risk jurisdiction/customers.
- SARs.
- Investigative court orders received.
- AR relationships exited due to financial crime reasons.

13.4 Notifications to the FCA

The Firm is required to complete an annual attestation of the accuracy of its FCA register details within 60 days of its accounting reference date via Connect and either confirm no changes or make appropriate changes. However, changes to such details should be made on a timely basis during the annual period in any case, normally in advance, to ensure that FCA register details remain up to date.

The Firm is also required to submit an annual attestation on Certified staff (entitled Directory persons), similarly making any changes or confirming no changes required. This is required within every 12 months and for the Firm, this is done in March each year.

Otherwise, Principle 11 includes a requirement for the Firm to disclose to the FCA anything relating to the Firm of which the FCA would reasonably expect notice. Various chapters in the FCA Handbook (SUP 11, SUP 12.7, SUP 15) also contain specific event-driven notification requirements for FCA-regulated firms. The following list is not exhaustive, and staff should refer to the Compliance Officer or SUP 15 if in any doubt.

13.4.1 Notification of Changes in Control or Close Links

- The Firm should notify the FCA (and normally in advance) about certain changes in its controlling structure (e.g. a new entity/person acquiring control, acquiring an additional kind of control or reducing/ceasing to have control).

- A new controller or a controller moving to a higher control band requires advance notification and FCA consent. This is called a s.178 notice (this being covered by s.178 of FSMA). Specified forms are required depending on the legal status of the new/increased controller.
- The FCA should also be notified immediately when the Firm becomes aware that it has become or ceased to become closely linked with any person. SUP 11 sets out more information on this.

13.4.2 Auditors

- Change of auditors.
- If a qualified audit report is expected.
- Written communication received from the Firm's auditors with regards to internal controls.

13.4.3 The Firm's Regulated Business Activities

- Any intention to vary or cease the regulated activities the Firm undertake.
- Change of the Firm's accounting reference date.
- The Firm intends to cancel its Part 4A permission.
- The Firm intends to wind down (run off) its activities.
- The Firm appoints or terminates an AR.

13.4.4 Matters Having a Serious Regulatory Impact

- The Firm not being able to maintain its capital resources requirement.
- The Firm fails to satisfy one or more of the threshold conditions, either as a result of its own actions, or that of any of its ARs.
- Legal action against any of its controllers.
- Any matter which could have a significant adverse impact on the Firm's reputation.
- Any matter which could affect the Firm's ability to continue to provide adequate services to the Firm's clients and which could result in a serious detriment to a client of the Firm.
- Any matter in respect of the Firm, which could result in serious financial consequences to the UK financial system or to other regulated firms.

13.4.5 Breaches of Rules or FSMA Requirements

- A significant breach of a rule (which includes a Principle or Statement of Principle, or a COCON rule).
- A breach of any requirement imposed by the Act (FSMA) or by regulations or an order made under the Act by the Treasury.
- The bringing of a prosecution for, or a conviction of, any offence under the Act by (or against) the Firm, controllers, or any of its staff members, or ARs.

Any breach notification should include information about any circumstances relevant to the breach or offence, identification of the rule or requirement, and any action which the Firm has taken or intends to take to rectify or remedy the breach or prevent any future potential occurrence.

The SM&CR imposes strict reporting requirements on firms for Conduct Rule breaches that result in disciplinary action. Disciplinary action in this context means:

- Issuing of a formal written warning.
- Suspension or dismissal of a person.
- Reduction or recovery of remuneration (clawback).

Where the disciplinary action is against an SMF holder, firms are required to notify the FCA within 7 business days of concluding disciplinary action using Form D (or Form C where the individual will no longer be approved).

Where the disciplinary action is against an individual other than an SMF holder, the FCA requires firms to notify annually through RegData using REP008. It is anticipated that the Firm will need to submit this report each October for the period 1 September to 31 August.

The Firm needs to make an annual notification about Conduct Rules even if there have not been any breaches to make sure it is correctly monitoring and identifying Conduct Rule breaches.

13.4.6 Civil, Criminal or Disciplinary Proceedings Against the Firm

- Civil proceedings against the Firm, whereby the amount of the claim is significant in relation to the Firm's financial resources or reputation.
- Any action that is brought against the Firm under section 71 or section 150 of FSMA (Action for damages).
- Disciplinary measures or sanctions that have been imposed on the Firm by any statutory or regulatory authority, professional organisation or trade body (other than the FCA) or the Firm becomes aware that one of those bodies has started an investigation into the Firm's affairs.
- If the Firm is prosecuted for, or convicted of, any offence involving fraud or dishonesty, or any penalties imposed on it for tax evasion.

Notification should include details of the matter and an estimate of the likely financial consequences, if any.

13.4.7 Fraud, Errors and Other Irregularities Provided they are Significant

- If the Firm become aware that a staff member may have committed a fraud against one of the Firm's clients.
- If the Firm become aware that a person, whether or not employed by the Firm, may have committed a fraud against the Firm.
- If the Firm identify irregularities in the Firm's accounting or other records, whether or not there is evidence of fraud.
- If the Firm expect that one of the Firm's staff members may be guilty of serious misconduct concerning their honesty or integrity and which is connected with the Firm's regulated activities or ancillary activities.

13.4.8 Change in Name or Address

- Change of the Firm's name or any other business name under which the Firm carry out regulated or ancillary activities either from an establishment in the UK or with or for clients in the UK (given with reasonable advance notice).
- Change in name or address of any of its ARs.
- Change in the Firm's principal place of business in the UK including date of the change (given with reasonable advance notice).

13.4.9 Change in Legal Status

- Please note, given that Part 4A permission is not transferable, a change in legal status will likely require an entirely new application to the FCA for Part 4A permission.

Notifications are, to a large extent, left to the discretion of regulated firms. However, the FCA has issued guidance as to what such notifications may comprise. The FCA expects firms to discuss relevant matters with it at an early stage, before making any internal or external commitments.

The Compliance Officer is responsible for providing any notifications from the Firm to the FCA or, in their absence, a member of the Governing Body. All information provided in a notification must be factually accurate and complete or, in the case of estimates and judgements, fairly and properly based after appropriate enquiries have been made. If the Firm becomes aware that it has or may have provided the FCA with information which was, or may have been false, misleading, incomplete, inaccurate or may have materially changed, it must notify the FCA immediately.

13.5 Major Share Holding Disclosure

DTR 5 requires shareholders to disclose holdings in certain shares once they reach, exceed or fall below defined thresholds. Special Rules, DTR 5.1.5, apply to FCA Authorised Persons that manage investments on behalf of beneficial owners.

The Firm, as an investment manager, may from time to time be obliged to disclose to both the FCA and to the issuer of the share, when relevant holdings reach, exceed or fall below the thresholds for relevant shares of UK issuers at 5% and 10% and every 1% thereafter.

13.5.1 How This Applies to Contracts for Difference

The contracts for difference (CFDs) disclosure costs apply to CFDs where the 'underlying' (i.e. the financial instrument upon which the CFD's value is determined) is admitted to trading on a UK prescribed market (i.e. UK regulated markets and AIM).

Firms have to report 'effective economic value of CFD holding' on a delta adjusted basis.

13.5.2 Definitions

- Relevant holdings – the aggregate of any voting rights held as a percentage of total voting rights conferred by that relevant share's issued share capital.
- Relevant shares – shares admitted to trading on a prescribed market (that include regulated markets, i.e. within the EEA).
- UK issuer – an issuer who is incorporated in the UK and whose shares are admitted to trading on a regulated market and their home state is the UK.
- Non-UK issuer – an issuer who is not incorporated in the UK and whose shares are admitted to trading on a regulated market and their home state is the UK.
- Regulated market – as defined by MiFID a list of regulated markets is maintained by CESR.
- Currently, prescribed markets include AIM which is the only market that is not also a regulated market.

13.5.3 Means of Disclosure

All relevant forms and checklists for Listing Transactions and Primary Market Oversight forms, including Form TR-1 (plus annex, where appropriate) for shares admitted to trading on a UK regulated market or prescribed market, are available on the FCA's website here. However, from 22 March 2021, all TR-1 notifications in relation to voting rights held in an issuer admitted to trading on a UK regulated market, must be submitted to the FCA via the major shareholdings notification portal via the FCA's electronic submission system (ESS).

To be able to submit a notification to the FCA, a relevant person (i.e. subject to notification obligations under DTR 5 and persons reporting TR-1 Forms on behalf of Position Holders (Reporting Persons) must complete a 2-step registration process on the ESS.

More information, including on the registration and form submission processes, are available on the FCA's website here.

13.5.4 Timing of Disclosure

- Shares issued by UK issuers:
    - To the issuer; as soon as possible but no later than within 2 trading days of the purchase/sale in the event the relevant holding reaches, breaches or falls below a threshold.
    - To the FCA; as soon as possible but no later than the end of the following trading day of the purchase/sale in the event the relevant holding reaches, breaches or falls below a threshold.
- Shares issued by non-UK issuers:
    - To the issuer; as soon as possible but no later than within 4 trading days of the purchase/sale in the event the relevant holding reaches, breaches or falls below a threshold.
    - To the FCA; as soon as possible but no later than the end of the second trading day of the purchase/sale in the event the relevant holding reaches, breaches or falls below a threshold.

13.5.5 Responsibility to Disclose

It is the responsibility of the Compliance Officer to make the disclosure regarding relevant major shareholdings as required by DTR 5.

13.6 Transaction Reporting

13.6.1 Transaction Reporting

SUP 17A and MiFIR Article 26 requires that a firm which 'executes' with a trading venue (i.e. regulated market, MTF, OTF or third-country trading venue) either directly or transmitted through a third party, a transaction in any reportable (as defined) financial instrument, must report the details of the transaction to the FCA in an accurate, timely and complete manner.

This only applies where the Firm is executing or managing investments either on its own behalf for 'direct' clients or any of its ARs. Therefore, it does not apply to advisory or arranging activities carried out by ARs in their own capacity as the obligation will fall on other parties to the transaction if in scope.

At present the activities of the Firm and its ARs are not in scope, as they are not being executed on any of the above 'venues' including a trading venue. Therefore, SUP 17A. does not apply to any of the Firm's or ARs' activities.

If, however, that were to change, the Firm is required to follow the procedures under SUP 17A.1 including:

- Either registering with the FCA to submit these reports directly and in line with SUP 17A.2.
- Or by way of using a third-party approved reporting mechanism (ARM) (for which FCA authorisation for that activity is required by the third party).

In practice if the Firm's activities were in scope of transaction reporting, it would appoint a recognised ARM (after appropriate due diligence) to carry out this reporting on its behalf.

Such reporting post MiFIR includes up to 65 data fields including (but not exclusive to):

- The time and date of a transaction.
- The securities involved with relevant identifiers.
- The price and volume.
- Specific identifiers on the trader/dealer/manager taking responsibility for the transaction.

All trades must be reported on a transaction date (T) +1 basis and any errors or omissions in compliance with this are required to be reported to the FCA's Market Reporting Team in line with their guidance at any given time. SUP 15 notification should also be considered on a proactive basis if the reason for a failure is due to any systemic issue.

Although the Firm may appoint an ARM to carry out reporting on its behalf, the obligation remains with the Firm regarding completeness, timeliness and accuracy of the submission. Therefore, confirmation of the successful submission from the ARM to the FCA on each and every transaction should be evidenced by the Firm as part of its audit trail on in-scope transactions. This should also include that the transaction has been carried out in line with reporting deadlines.

The FCA also encourages firms to sign up to its Market Data Portal (MDP), which enables a firm to obtain extracts of reports submitted directly from the FCA for independent sampling. Should this be required, the Firm undertakes to sign up to the MDP as part of its ongoing monitoring programme and in line with SUP 17A.2.1B.

13.7 Mandatory Notifications under the NSI Act 2021

The UK's National Security and Investment Act 2021 (NSI Act) received Royal Assent in April 2021 and came into force on 4 January 2022. The NSI Act introduced a hybrid mandatory and voluntary notification regime enabling the government to scrutinise and intervene in certain transactions and investments on national security grounds.

As set out on the government's website here, the NSI Act permits the government to impose certain conditions on an acquisition, or in rare instances, the government may unwind or block an acquisition completely.

In general, the new regime will apply to any acquisition of 'material influence' in a qualifying entity, which is widely defined as any entity other than an individual, as well as the acquisition of control over assets (including land and intellectual property), which are from, in, or have a connection to the UK, and which potentially give rise to national security concerns in the UK. It is worth noting that qualifying acquisitions that are part of a corporate restructure or reorganisation may also be covered.

The government has published a flowchart to help relevant persons decide whether an acquisition needs to be notified.

13.7.1 Mandatory Notifications

A mandatory notification from the acquirer applies to notifiable acquisitions in 17 key sectors (listed below), which are defined in the NSI Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021 (accessible here):

1. Advanced Materials
2. Advanced Robotics

3. Artificial Intelligence
4. Civil Nuclear
5. Communications
6. Computing Hardware
7. Critical Suppliers to government
8. Cryptographic Authentication
9. Data Infrastructure
10. Defence
11. Energy
12. Military and Dual-Use
13. Quantum Technologies
14. Satellite and Space Technologies
15. Suppliers to the Emergency Services
16. Synthetic Biology
17. Transport

Section 8 of the NSI Act sets out 4 cases (or trigger events) where control of a qualifying entity would require mandatory notification to the Investment Security Unit (ISU) within the Department for Business, Energy and Industrial Strategy (BEIS) and approval by the Secretary of State for BEIS before it completes:

1. The first case is where the percentage of the shares that the person holds in the entity increases:
   (a)from 25% or less to more than 25%,
   (b)from 50% or less to more than 50%, or
   (c)from less than 75% to 75% or more.
2. The second case is where the percentage of the voting rights that the person holds in the entity increases:—
   (a)from 25% or less to more than 25%,
   (b)from 50% or less to more than 50%, or
   (c)from less than 75% to 75% or more.
3. The third case is where the acquisition is of voting rights in the entity that (whether alone or together with other voting rights held by the person) enable the person to secure or prevent the passage of any class of resolution governing the affairs of the entity.
4. The fourth case, subject to section 9 of the NSI Act, is where the acquisition, whether alone or together with other interests or rights held by the person, enables the person materially to influence the policy of the entity.

13.7.2 Qualifying Acquisition of an Asset

For the purposes of the NSI Act and subject to the exceptions set out in section 11, a person gains control of a qualifying asset if the person acquires a right or interest in, or in relation to, the asset and as a result the person is able:

a) To use the asset, or use it to a greater extent than prior to the acquisition, or
b) To direct or control how the asset is used, or direct or control how it is used to a greater extent than prior to the acquisition.

Qualifying acquisitions are not subject to mandatory notification but may be subject to a ‘call in notice’.

13.7.3 Voluntary Notifications

If a qualifying acquisition is not in scope of the mandatory notification there is no legal obligation to tell the government about it. However, a voluntary notification can be submitted if a party to the transaction wants to know if the government will call it in for review.

In the case of a voluntary notification, the acquisition may continue unless the government has said otherwise through an interim order. However, if the acquisition completes before the government has made its decision, the acquisition can later be unwound if the government finds that there are national security concerns.

13.7.4 Procedure to Notify

To tell the government about a notifiable acquisition, an online mandatory notification form needs to be submitted online to the Investment Security Unit. Before a form can be submitted, registration for the online service is required. The form asks for information on the structure and share ownership of the qualifying entity, the acquirer and the acquisition. Further guidance on how to submit a notification form is here.

Two other notification forms are also available: voluntary notifications and retrospective validation application form. The latter form is for retrospective validation if a notifiable acquisition has completed without notifying. However, as set out below, an acquisition is void if a notifiable acquisition (which is subject to mandatory notification) completes without notifying and gaining approval from the government, and civil and criminal action may also result.

After a notification form has been submitted, the government will provide a case reference number and will confirm whether the form has been accepted or rejected as soon as is reasonably practicable after receiving it. The acquisition can continue to progress using the review and assessment periods up to the point of completion unless the government has issued an interim order preventing this.

If the notification form is accepted, within 30 working days the government will either:

- Clear the acquisition and confirm it can go ahead.
- Clear the acquisition to go ahead subject to certain conditions.
- 'Call in' the acquisition for a full national security assessment, which will last up to 30 days, subject to extensions of up to 45 working days.
- Require further information, which should be provided as soon as possible, to help complete the assessment (known as an 'information notice').
- Require a party or various parties involved in the acquisition to attend a meeting (known as an 'attendance notice').

More information on the assessment procedure can be found here.

13.7.5 Call in Powers

The government can assess acquisitions up to 5 years after they have taken place and up to 6 months after becoming aware of them if they have not been notified.

To avoid parties rushing through transactions, the government has reserved the right to apply the provisions of the NSI Act retrospectively for transactions completing between 12 November 2021 and 3 January 2022.

13.7.6 Enforcement

Completing a notifiable acquisition without approval will mean the acquisition is legally void and may mean that the acquirer is subject to civil or criminal penalties including up to 5 years in prison and/or a fine of up to the greater of 5% of an organisation's global turnover or £10m, whichever is the greater.

The Act also contains offences for:

- Failing to comply with an interim or final order.

- Failing to comply with an information notice or attendance order, and various associated offences.
- Using or disclosing information in contravention of disclosure of information provisions.

13.7.7 Extra-territorial effects of the NSI Act

Under the NSI Act, there are new rules that apply to certain acquisitions of entities or assets that are outside, but have a connection to, the UK.

The guidance here explains:

- What type of acquisitions outside of the UK are covered by the new rules.
- Common circumstances that would put an acquisition in scope of the new rules.
- Examples of how the rules may affect parties not based in the UK.

13.7.8 Further Information and Assistance on the NSI Act

For general enquiries or for an informal discussion around future acquisitions or a specific notification, please contact the ISU at investment.screening@beis.gov.uk.