Contents

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 4.1 General Requirements.

3.2 Allocation of Responsibilities and Oversight

Following the FCA outcomes-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 covering their 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 the FCA's Senior Management and Certification Regime (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.

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, which 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.
- Clear allocation and ownership of risks amongst the Senior Management Group (of SMF Holders) documented in the Firm's business-wide risk register, which is reviewed quarterly.
- 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, 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 Firm's Partners 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 are established, and the appropriate individuals will be obliged to provide updates to the Governing Body at these meetings. The meetings are 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 Partners will maintain organisational charts which clearly specify reporting lines and allocate functions, PRs and other responsibilities, however, ultimate responsibility for the governance arrangements of the Firm remains at Partner level regardless of any delegation of tasks. 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.
- The senior management group, which includes all SMF holders (partners, the Compliance Officer and the MLRO), holds a quarterly risk register review meeting to discuss existing risks and any new risks that have been added to the pending tab for that quarter. This includes ongoing assessment or any change of risk rating based on impact and probability of the event taking place. The Firm's AR size metrics tracker is also updated prior to the quarterly meeting for discussion during the meeting. Once changes are agreed, the Compliance Officer implements the updates and prepares the register for the next quarterly review.
- Risks are given specific references and are allocated to the most suitable member of senior management based on senior management role profiles and areas of responsibility. However, all risks are reviewed by all members of senior management every quarter.

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 Partners 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 where relevant, the FCA, the ICO, ARs, insurers, 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 MLRO will update the BCP whenever there is a material change to the Firm's operations, structure including staff, business, location or regulations. In addition, the BCP will be regularly reviewed and periodically tested. The Firm's Founding Partner has ultimate responsibility for the Firm's BCP.

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 to the Firm's Founding Partner, Kevin Gallacher with assistance from the MLRO. The Founding Partner is ultimately responsible for data security arrangements within the Firm. However, external notifications, where required, are actioned either by the Compliance Officer or the MLRO depending upon the reason and nature of the notification.

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 and all relevant recommendations made by its third-party IT consultants.

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.
- All staff are required to use strong passwords, which should be changed periodically, and to use/enable multiple factor authentication,
- 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 and termination/off-boarding procedures 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 without delay.
- 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. Confidentiality requirements are reflected in contracts for services with staff.

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 7 core principles and their implementation are set out below:

1. **Lawfulness, Fairness and Transparency** – the Firm only holds data it is required to hold to comply with FCA or business requirements and data subjects have the right to request their data at any time.
2. **Purpose Limitation** – the Firm only holds data it is required to hold to comply with FCA or business requirements and does not use this data for any other purpose.
3. **Data Minimisation** – the Firm only holds data it is required to hold to comply with FCA and legal requirements.
4. **Accuracy** – the data subject has the right to request a copy of their data at any time and for it to be rectified if required.
5. **Storage Limitation** – the Firm will only hold on to the data for the period it is legally required.
6. **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.
7. **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 or data map 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 firm's Founding Partner 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. The requirement to comply with regulatory requirements for record keeping may also supersede any such request.

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.

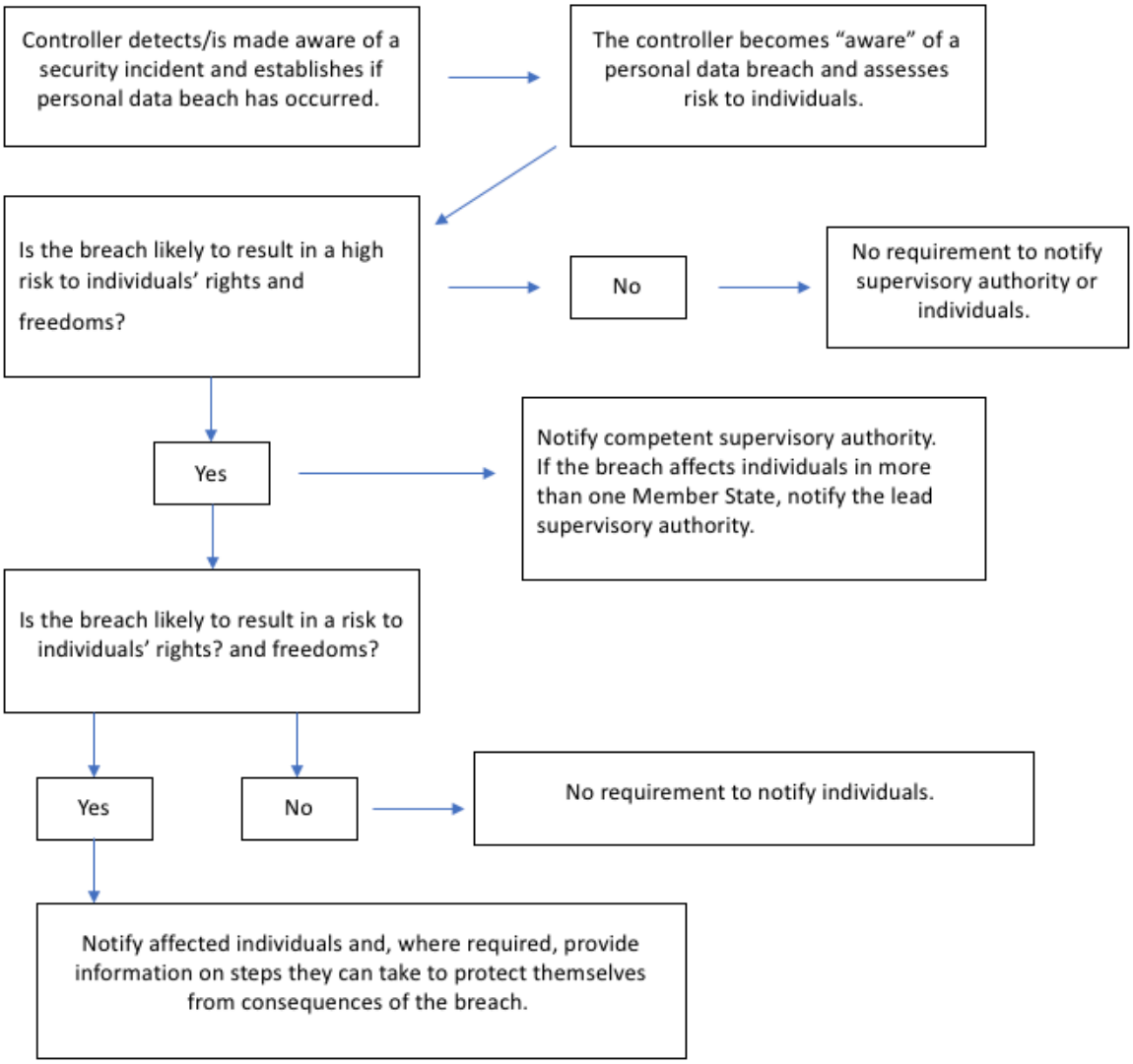
3.7.2 Personal Data Breach Notification

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 use 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 not of a 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 person internally responsible for Data Protection 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 the data. 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 MLRO 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 of FCA-regulated firms, to carry out a formal audit of its accounts at least annually and prepare quarterly VAT returns. 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 Prudential Requirements and any Individual Capital Guidance. 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 are 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. If 2 employment references are not available, appropriate alternatives including from professional firms or bodies or personal references may be considered. 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. An entry in the conflicts of interest register will also be made where an individual is known to existing staff members.

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. Further information on this is covered in Chapter 5 of the Manual.

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. The Firm should also take into account any regulatory guidance on expectations of effective compliance functions including current guidance from ESMA.

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's responsibilities include monitoring and assessing the effectiveness of the compliance procedures and taking action, with agreement from the Firm's Partners, 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.

The Firm also engages with Gem Compliance Consulting Ltd, which is a member of the Association of Professional Compliance Consultants, and an established 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 independence, 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.
6. Responsibility for relevant, assigned risks in the Firm's business-wide risk register.

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, number of staff members and simple business operations, the Firm's Compliance Officer may be involved in associated operational tasks. 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 tasks they become involved in.

3.13.2 Internal Audit

SYSC 6.2.1 R requires that where considered appropriate and proportionate, a firm should 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 Adequacy and Risk Assessment (ICARA) process. It may also use other risk management tools and records where necessary. Ultimately, it is the responsibility of the Partners to maintain appropriate risk management arrangements along with the Compliance Officer and the MLRO. 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 process (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 normally paid by Standing Order, 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 not act as a counterparty in any investment transaction 'chain' (where one exists) between its ARs, Funds and the ARs' underlying clients i.e. investors. 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 directly 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, fraud etc.

These risks are assessed in the ICARA process 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 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, personnel 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), that

there is a valid, written agreement in place which clearly allocates and sets out rights and responsibilities, and which ensures effective performance against agreed standards, e.g. service level agreement, that there is regular review and monitoring of the relationship and activities carried out by the service provider, that there is a process in place for 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. Conduct due diligence prior to engagement.
2. Retain expertise to supervise and manage effectively.
3. Take action if problems appear.
4. Have power to terminate the outsourcing agreement without detriment to client service.
5. 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, prior to the 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 and cannot be altered.

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/retention 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 (and ARs) 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 interest 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. However, ARs should also be maintaining their own conflicts of interest registers on Leo, the compliance platform Midmar uses.

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 or software/apps 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.

This applies to both MiFID and AIFM management activities. This includes where the financial instrument is a transferable security (as defined) which can include unlisted equities. However the Firm is exempt from these requirements where such investments are not traded on public markets which is currently the case for the Firm's investment activities.

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

- Date and time of meetings.
- Location of meetings.
- Identity 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.

All external business-related communications (verbal and written) should be on company-owned devices and only delivered using company-approved software, which can be interrogated where required, e.g. in response to a data subject access request. Personal devices may only be used in accordance with the Firm's/AR's personal devices 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's Compliance Officer before becoming a partner, director, officer or adviser in an outside organisation, regardless of whether or not it is a paid position.

The approval 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 (in the case of Firm staff) nor shall it conflict or interfere with the main business of the Firm or the relevant AR in any way.

The Firm and AR 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. An annual Outside Business Interests Attestation will also be required from all Firm and relevant AR staff.

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 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 and Speaking Up

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. bribery, or failure of the Firm to prevent bribery on its behalf.
    - 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 initially to a designated partner unless the particular concern involves the 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 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 between 10am to 3pm, or a message can be left.
- FCA's direct email address is whistle@fca.org.uk
- FCA's online form
- 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
Webform
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.