SYSC

Table of Contents

Navigating SYSC

The purposes of SYSC are: (1) to encourage firms' directors and senior managers to take appropriate practical responsibility for their firms' arrangements on matters likely to be of interest to the FCA because they impinge on the FCA's functions under the Act; (2) to increase certainty by amplifying Principle 3, under which a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems; (3) to encourage firms to vest responsibility for effective and responsible organisation in specific

directors and senior managers; and (4) to create a common platform of organisational and systems and controls requirements for all firms.

SYSC 1 guides the reader through the application of SYSC rules - particularly what rules apply to different types of firms. SYSC 2 deals with apportionment of responsibilities. Here, senior managers are expected to have clarity on their responsibilities and in such a way that the business and affairs of the firm can be controlled, monitored and governed adequately.

Systems and Controls - SYSC 3

A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business. The nature and extent of the systems and controls which a firm will need to maintain will depend upon a variety of factors including: (a) the nature, scale and complexity of its business; (b) the diversity of its operations, including geographical diversity; (c) the volume and size of its transactions; and (d) the degree of risk associated with each area of its operation. To enable it to comply with its obligation to maintain appropriate systems and controls, a firm should carry out a regular review of them.

What does the FCA consider to be appropriate systems and controls?
Appropriate systems and controls include systems and controls around the following

- Skills Knowledge and expertise
- Governance
- Organisation of systems and control of the business
- Compliance including financial crime and AML
- Risk Assessment function
- The use of Management Information’
- Employee and Agents systems
- Audit Committee
- The internal Audit function
- Requirements around business strategy
- Remuneration policies
- Business Continuity

- Records
- Investment strategy and decision making

Governance

UK Corporate Governance code is relevant for companies who have a Premium Listing of equity shares in the UK . These companies are required under the Listing Rules to report in their annual report and accounts on how they have applied the Code.
This responsibility includes responsibilities to tied agents and appointed representatives.

Skills, knowledge and expertise

A firm must employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them. When complying with the competent employees rules, a firm must take into account the nature, scale and complexity of its business and the nature and range of financial services and activities undertaken in the course of that business.
SYSC 28 contains rules and guidance relating to the minimum knowledge and competence requirements in relation to insurance distribution activities undertaken by a firm. The Training and Competence sourcebook (TC) contains additional rules and guidance relating to specified retail activities undertaken by a firm. Firms which are carrying on activities that are not subject to TC may nevertheless wish to take TC into account in complying with the competence requirements in SYSC.

Organising systems and controls

A firm's reporting lines should be clear and appropriate having regard to the nature, scale and complexity of its business. These reporting lines, together with clear management responsibilities, should be communicated as appropriate within the firm. (1) A firm's governing body is likely to delegate many functions and tasks for the purpose of carrying out its business. When functions or tasks are delegated, either to employees or to appointed representatives or, where applicable, its tied agents, appropriate safeguards should be put in place. (2) When there is delegation, a firm should assess whether the recipient is suitable to carry out the delegated function or task, taking into account the degree of responsibility involved. (3) The extent and limits of any delegation should be made clear to those concerned. (4) There should be arrangements to supervise delegation, and to

monitor the discharge of delegates functions or tasks. (5) If cause for concern arises through supervision and monitoring or otherwise, there should be appropriate follow-up action at an appropriate level of seniority within the firm.

The guidance relevant to delegation within the firm is also relevant to external delegation ('outsourcing'). A firm cannot contract out its regulatory obligations.
So, for example, under Principle 3 a firm should take reasonable care to supervise the discharge of outsourced functions by its contractor. (2) A firm should take steps to obtain sufficient
information from its contractor to enable it to assess the impact of outsourcing on its systems and controls. Where it is made possible and appropriate by the nature, scale and complexity of its business, a firm should segregate the duties of individuals and departments in such a way as to reduce opportunities for financial crime or contravention of requirements and standards under the regulatory system. For example, the duties of front-office and back-office staff should be segregated so as to prevent a single individual initiating, processing and controlling transactions.

Compliance

A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime. A firm must ensure that these systems and controls:

1. enable it to identify, assess, monitor and manage *money laundering* risk; and
2. are comprehensive and proportionate to the nature, scale and complexity of its activities.

"Money laundering risk" is the risk that a firm may be used to further money laundering. Failure by a firm to manage this risk effectively will increase the risk to society of crime and terrorism.

A *firm* must carry out regular assessments of the adequacy of these systems and controls to ensure that it continues to comply with *the compliance rule above.* In identifying its *money laundering* risk and in establishing the nature of these systems and controls, a *firm* should consider a range of factors, including:

1. its customer, product and activity profiles;
2. its distribution channels;
3. the complexity and volume of its transactions;
4. its processes and systems; and
5. its operating environment.

Systems and Controls

A firm should ensure that the systems and controls include:

1. appropriate training for its employees in relation to money laundering;
2. appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's money laundering reporting officer (MLRO) on the operation and effectiveness of those systems and controls;
3. appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies
4. appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:
    1. (a) the development of new products;
    2. (b) the taking-on of new customers; and
    3. (c) changes in its business profile.

The Money Laundering Reporting Officer (MLRO)

The job of the MLRO within a firm is to act as the focal point for all activity within the firm relating to anti-money laundering. The FCA expects that a firm's MLRO will be based in the United Kingdom.

Risk Assessment function.

This is a function that is required by the PRA for Solvency II firms. Its role is to assess a company's risks and advice on them. It also involves the setting of and controlling risk exposure.

Management Information System

A firm’s arrangements should be such as to furnish its governing body with the information it needs to play a part in identifying, measuring and controlling risks of regulatory concern.
Management information is needed for key risks such as fair treatment of customers, Consumer protection, Effective competition, Integrity of the UK financial system.
E.g of Management information includes - Number of new clients, kyc checks. failed sanction checks, SARS made. These can be used to monitor changes in the control environment such as the increasing or decreasing levels of risk and turnaround of services in the firm.

Employees and Agents

Firms are expected to assess the suitability of anyone who acts for it. This includes assessments of honesty and competence and suitability for responsibilities and roles. This is usually done at recruitment.

Audit Committee

The requirement for this depends on the nature scale and complexity of the business. It is recommended for larger firms, as part of the governance frameworks. Listed firms are often required

to have this. Their remit includes the examination of management processes for ensuring effective/ appropriate controls and it oversees the internal audit function.

Internal Audit

Also depends on the nature, scale and complexity of business. Its function is to assess the adherence to and the effectiveness of internal controls (e.g policies and procedures) within a firm. Solvency II firms are required to have an internal audit function (team of internal auditors) as well as a Chef Internal Audit function.

Business Continuity

This refers to the need to have appropriate arrangements to ensure that a business can continue to function and meet its regulatory obligations in the event of unforeseen interruption. This is an arrangement that deals with the deployment of alternative systems, such as working from home or remotely, communication of these systems with relevant staff and contractors as well as managing the infrastructure through which this can be done. I.e - The IT system for remote working.

Records

The rulebook requires that reasonable care must be taken to make records of matters / dealings subject to regulatory requirements. Records are expected to be retained for as long as is relevant for the purposes for which the records were created.

1. A common platform firm must arrange for records to be kept of all services, activities and transactions undertaken by it.
2. The records referred to above must be sufficient to enable the FCA to fulfil its supervisory tasks and to perform the enforcement actions under the regulatory system including MiFID, MiFIR and the Market Abuse Regulation, and in particular to ascertain that the common platform firm has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market.

Investment Strategy and Decision making

The regulator expects that ESG and other financial information may play a role in the considerations made when formulating strategy and when making investment decisions. Financial considerations include interest rates, liquidity, concentration, exchange rates, political and counterparty risks. Non

financial matters are considered only when shareholders share the same view and / or it involves no risk of financial detriment.

Governance - General requirement.

A firm must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems.

Data Security Requirements

A *common platform firm* must have sound security mechanisms in place for the following, while maintaining the confidentiality of the data at all times:

1. (a) to guarantee the security and authentication of the means of transfer of information;
2. (b) to minimise the risk of data corruption and unauthorised access; and
3. (c) to prevent information leakage.

Mechanisms and procedures for a firm - SYSC 4.1.4

A firm (with the exception of a common platform firm and a sole trader who does not employ any person who is required to be approved under section 59 of the Act (Approval for particular arrangements)) must, taking into account the nature, scale and complexity of the business of the firm, and the nature and range of the financial services, claims management services and other activities undertaken in the course of that business: frms must

1. establish, implement and maintain decision-making procedures and an organisational structure which clearly and in a documented manner specifies reporting lines and allocates functions and responsibilities;
2. establish, implement and maintain adequate internal control mechanisms designed to secure compliance with decisions and procedures at all levels of the *firm*;

3. establish, implement and maintain effective internal reporting and communication of information at all relevant levels of the *firm*; and
4. establish, implement and maintain effective internal reporting and communication of information at all relevant levels of the *management company* as well as effective information flows with any third party involved.

Business continuity - SYSC 4.1.6

A common platform firm must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities. To this end the common platform firm must employ appropriate and proportionate systems, resources and procedure

A UK bank, building society and an investment firm and a management company must establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to its systems and procedures, that any losses are limited, the preservation of essential data and functions, and the maintenance of its regulated activities, or, in the case of a management company, its collective portfolio management activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of those activities.

The matters dealt with in a business continuity policy should include:

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*, *clients* and the press);
4. escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;
5. processes to validate the integrity of information affected by the disruption; and
6. regular testing of the business continuity policy in an appropriate and proportionate manner

Accounting policies and procedures - SYSC 4.1.9

A management company must establish, implement and maintain accounting policies and procedures that enable it, at the request of the *FCA*, to deliver in a timely manner to the *FCA* financial reports which reflect a true and fair view of its financial position and which comply with all applicable accounting standards and rules.

Regular monitoring: management company - SYSC 4.1.10

A management company must monitor and, on a regular basis, evaluate the adequacy and effectiveness of its systems, internal control mechanisms and arrangements established in accordance with all of the above rules and take appropriate measures to address any deficiencies.

Responsibility of senior personnel - SYSC 4.3

A *firm* (with the exception of a *common platform firm* and a *sole trader* who does not employ any approved *person*), when allocating functions internally, must ensure that *senior personnel* and, where appropriate, the *supervisory function*, are responsible for ensuring that the *firm* complies with its obligations under the *regulatory system*. In particular, *senior personnel* and, where appropriate, the *supervisory function* must assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the *firm's* obligations under the *regulatory system* and take appropriate measures to address any deficiencies

A *firm* that is a *management company* or Debt Collecting Firm must ensure that:

1. Its *senior personnel* receive on a frequent basis, and at least annually, written reports on the matters covered by *compliance, internal audit, risk control and financial crime* indicating in particular whether the appropriate remedial measures have been taken in the event of any deficiencies; and
2. The *supervisory function*, if any, receives on a regular basis written reports on the same matters.

Other *firms* should take account of the written reports *rule* (*SYSC 4.3.2 R*) as if it were *guidance* (and as if "should" appeared in that *rule* instead of "must") as explained in *SYSC 1 Annex 1* 3.

The *supervisory function* does not include a general meeting of the shareholders of a *firm*, or equivalent bodies, but could involve, for example, a separate supervisory board within a two-tier board structure or the establishment of a non-executive committee of a single-tier board structure.

Management body governance - SYSC 4.3A

Management body

A *common platform firm* must ensure that the *management body* defines, oversees and is accountable for the implementation of governance arrangements that ensure effective and prudent management of the *firm*, including the segregation of duties in the organisation and the prevention of conflicts of interest, and in a manner that promotes the integrity of the market and the interests of *clients*.

The *firm* must ensure that the *management body*:

1. has overall responsibility for the *firm*;
2. approves and oversees implementation of the *firm's* strategic objectives, risk strategy and internal governance;
3. ensures the integrity of the *firm's* accounting and financial reporting systems, including financial and operational controls and compliance with the *regulatory system*.
4. oversees the process of disclosure and communications;
5. has responsibility for providing effective oversight of *senior management*;
6. monitors and periodically assesses:

1. (a) the adequacy and the implementation of the *firm's* strategic objectives in the provision of *investment services and/or activities* and *ancillary services*;
2. (b) the effectiveness of the *firm's* governance arrangements; and
3. (c) the adequacy of the policies relating to the provision of services to *clients*, and

7. takes appropriate steps to address any deficiencies; and
8. has adequate access to information and documents which are needed to oversee and monitor management decision-making.

A *common platform firm* must ensure that the *management body* defines, approves and oversees:

1. The organisation of the *firm* for the provision of *investment services and/ or activities* and *ancillary services*, including the skills, knowledge and expertise required by personnel, the resources, the procedures and the arrangements for the provision of services and activities, taking into account the nature, scale and complexity of its business and all the requirements the *firm* has to comply with;
2. A policy as to services, activities, products and operations offered or provided, in accordance with the risk tolerance of the *firm* and the characteristics and needs of the *firm's clients* to whom they will be offered or provided, including carrying out appropriate stress testing, where appropriate; and
3. A remuneration policy of persons involved in the provision of services to *clients* aiming to encourage responsible business conduct, fair treatment of *clients* as well as avoiding conflict of interest in the relationships with *clients*

Firms must ensure that the members of the *management body* of the *firm*:

1. are of sufficiently good repute;
2. possess sufficient knowledge, skills and experience to perform their duties;
3. possess adequate collective knowledge, skills and experience to understand the *firm's* activities, including the main risks;
4. reflect an adequately broad range of experiences;
5. commit sufficient time to perform their functions in the *firm*; and
6. act with honesty, integrity and independence of mind to effectively assess and challenge the decisions of *senior management* where necessary and to effectively oversee and monitor management decision-making.

A *firm* should have procedures for monitoring the collective adequacy of the knowledge, skills and experience of its *management body* as well as of its individual members.

Apportionment of responsibilities - SYSC 4.4

A *firm* must take reasonable care to maintain a clear and appropriate apportionment of significant responsibilities among its *directors* and *senior managers* in such a way that:

1. it is clear who has which of those responsibilities; and
2. the business and affairs of the *firm* can be adequately monitored and controlled by the *directors*, relevant *senior managers* and *governing body* of the *firm*.

Allocating functions of apportionment and oversight

A *firm* must appropriately allocate to one or more individuals, in accordance with the following table, the functions of:

1. dealing with the apportionment of responsibilities and
2. overseeing the establishment and maintenance of systems and controls.

Competent employees rule - SYSC 5.1.1

A *firm* (other than a *common platform firm*) must employ personnel with the skills, knowledge and expertise necessary for the discharge of 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. 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.

SYSC 28 contains *rules* and *guidance* relating to the minimum knowledge and competence requirements in relation to *insurance distribution activities* undertaken by a *firm*.The Training and Competence sourcebook (*TC*) also contains additional *rules* and *guidance* relating to specified retail activities undertaken by a *firm. Firms* which are carrying on activities that are not subject to *TC* may nevertheless wish to take *TC* into account in complying with the competence requirements in *SYSC*.

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:

1. those *rules* which implement articles 24 and 25 of *MiFID* (including those *rules* which implement related provisions under the *MiFID Delegated Directive*); and
2. related provisions of the *MiFID Org Regulation*.

A *management company* must also ensure that its *relevant persons* are aware of the procedures which must be followed for the proper discharge of their responsibilities.

Compliance - Adequate policy and procedures - SYSC 6.1

A *firm* must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the *firm* including its managers, employees and *appointed representative*s (or where applicable, *tied agents*) with its obligations under the *regulatory system* and for countering the risk that the *firm* might be used to further *financial crime*.

Compliance function - SYSC 6.1.3

A *firm* that is a *management company* or Debt Collecting Firm must maintain a permanent and effective compliance function which operates independently and which has the following responsibilities:

1. to monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place in accordance with the compliance obligation, and the actions taken to address any deficiencies in the *firm's* compliance with its obligations; and
2. to advise and assist the *relevant persons* responsible for carrying out *regulated activities* to comply with the *firm's* obligations under the *regulatory system*.

The compliance function must have the necessary authority, resources, expertise and access to all relevant information. For management companies and operators of electronic systems, a compliance officer must be appointed and must be responsible for the compliance function and for any reporting as to compliance, the *relevant persons* involved in the compliance functions must not be involved in the performance of the services or activities they monitor and the method of determining the remuneration of the *relevant persons* involved in the compliance function must not compromise their objectivity and must not be likely to do so.

For most firms this means that they must allocate to a *director* or *senior manager* the function of: (a) having responsibility for oversight of the *firm's* compliance; and (b) reporting to the *governing body* in respect of that responsibilities.

Internal audit - SYSC 6.2.1

A firm that is a management company or Debt Collecting Firm or a management company must, where appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of its financial services and activities, undertaken in the course of that business, establish and maintain an internal audit function which is separate and independent from the other functions and activities of the firm and which has the following responsibilities:

1. to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the *firm's* systems, internal control mechanisms and arrangements;
2. to issue recommendations based on the result of work carried out in accordance with (1);
3. to verify compliance with those recommendations;
4. to report in relation to internal audit matters in accordance with *SYSC 4.3.2 R*.

Risk Control - SYSC 7.1

The *management body* of a *common platform firm* or of Debt Collecting Firm 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 which it operates in relation to the status of the business cycle.

For a *common platform firm* included with assets under management of over £250 million , the strategies, policies and procedures for identifying, taking up, managing, monitoring and mitigating the risks to which the *firm* is or might be exposed include conducting reverse stress testing in accordance with *SYSC 20*. Firms with less than £250 million assets under management should consider conducting reverse stress tests on its business plan as well. This would further *senior personnel's* understanding of the *firm's* vulnerabilities and would help them design measures to prevent or mitigate the risk of business failure.

A *firm* that is a *UCITS investment firm* or Debt Collecting Firm must monitor the following:

1. The adequacy and effectiveness of the *firm's* risk management policies and procedures;
2. The level of compliance by the *firm* and its *relevant persons* with the arrangements, processes and mechanisms adopted in accordance with the requirement
3. The adequacy and effectiveness of measures taken to address any deficiencies in those policies, procedures, arrangements, processes and mechanisms, including failures by the *relevant persons* to comply with such arrangements or processes and mechanisms or follow such policies and procedures.

Where a *firm* that is a *UCITS investment firm* or Debt Collecting Firm is not required to maintain a risk management function that functions independently, it must nevertheless be able to demonstrate that the policies and procedures which it has adopted satisfy the requirements of those *rules* and are consistently effective

Granting Credits

A *firm* must base credit-granting on sound and well-defined criteria and clearly establish the process for approving, amending, renewing, and re-financing credits. A *BIPRU firm* must operate through effective systems the ongoing administration and monitoring of its various credit risk-bearing portfolios and exposures, including for identifying and managing problem credits and for making adequate value adjustments and provisions.The firm must adequately diversify credit portfolios given its target market and overall credit strategy. The documentation maintained by a *BIPRU firm* should include its policy for credit risk, including its risk appetite and provisioning policy and should describe how it measures, monitors and controls that risk. This should include descriptions of the systems used to ensure that the policy is correctly implemented.

Residual risk

A *BIPRU firm* must address and control by means of written policies and procedures the risk that recognised credit risk mitigation techniques used by it prove less effective than expected.

Market risk

A *BIPRU firm* must implement policies and processes for the measurement and management of all material sources and effects of market risks.

Interest rate risk

A *BIPRU* firm must implement systems to evaluate and manage the risk arising from potential changes in interest rates as they affect a *BIPRUfirm's* non-trading activities.

Operational risk

A *BIPRU firm* must implement policies and processes to evaluate and manage the exposure to operational risk, including to low-frequency high severity events. Without prejudice to the definition of *operational risk*, *BIPRU firms* must articulate what constitutes operational risk for the purposes of those policies and procedures.

Risk Committee

A firm that is subject to the Capital Requirements Regulation (such as Banks and Investment Firms ("CRR Firms") and is significant must establish a risk committee composed of members of the management body who do not perform any executive function in the firm. Members of the risk committee must have appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and the risk appetite of the firm. This is relevant for firms such as Banks , Investment Firms.

1. The risk committee must advise the management body on the institution's overall current and future risk appetite and assist the management body in overseeing the implementation of that strategy by senior management.
2. The risk committee must review whether prices of liabilities and assets offered to clients take fully into account the *firm's* business model and risk strategy. Where prices do not properly reflect risks in accordance with the business model and risk strategy, the risk committee must present a remedy plan to the *management body*

A small Bank or Investment firm (Non IFPRU CRR Firms) may combine the risk committee with the audit committee. Members of the combined risk and audit committee must have the knowledge, skills and expertise required for both committees. A *CRR firm* must ensure that the *management*

body in its supervisory function and, where a risk committee has been established, the risk committee have adequate access to information on the risk profile of the *firm* and, if necessary and appropriate, to the risk management function and to external expert advice. The *management body* in its supervisory function and, where one has been established, the risk committee must determine the nature, the amount, the format, and the frequency of the information on risk which it is to receive.

The risk management function must ensure that all material risks are identified, measured and properly reported. It must be actively involved in elaborating the *firm's* risk strategy and in all material risk management decisions and it must be able to deliver a complete view of the whole range of risks of the *firm*.

A *CRR firm* must ensure that the risk management function is able to report directly to the *management body* in its supervisory function, independent from *senior management* and that it can raise concerns and warn the *management body*, where appropriate, where specific risk developments affect or may affect the *firm*, without prejudice to the responsibilities of the *management body* in its supervisory and/or managerial functions pursuant to the *CRD* and the *EU CRR*.

Credit institutions providing account information or payment initiation services - SYSC 9.2

A credit institution must keep records of any account information services and payment initiation services it provides. Records must be kept in respect of account information services and payment initiation services provided anywhere in the EEA. The records must make clear in which EEA State those services were provided.

The records must be sufficient to enable the *credit institution* to provide to the *FCA*, upon request, the following information:

1. The number of different payment accounts that the credit institution has accessed for the purposes of providing account information services.

2. The number of payment service users who have used the account information services provided by the credit institution.
3. The number of different payment accounts that the credit institution has accessed for the purposes of providing payment initiation services.
4. The number of payment transactions the credit institution has initiated when providing payment initiation services.
5. These records must be sufficient to enable the credit institution to provide the FCA with the information specified in SYSC 9.2.4R for each calendar year in the previous five years, except that there is no requirement to record this information for any period prior to 13 January 2018.

Chinese walls - SYSC 10.2

1. When a firm establishes and maintains a Chinese wall (that is, an arrangement that requires information held by a person in the course of carrying on one part of the business to be withheld from, or not to be used for, persons with or for whom it acts in the course of carrying on another part of its business) it may:
    1. (a) withhold or not use the information held; and
    2. (b) for that purpose, permit persons employed in the first part of its business to withhold the information held from those employed in that other part of the business;
2. but only to the extent that the business of one of those parts involves the carrying on of regulated activities, ancillary activities or, in the case of MiFID business, the provision of ancillary services.
3. Information may also be withheld or not used by a firm when this is required by an established arrangement maintained between different parts of the business (of any kind) in the same group. This provision does not affect any requirement to transmit or use information that may arise apart from the rules in COBS..

Obligations for telephone and electronic communications SYSC 10 A

A *firm* must take all reasonable steps to record telephone conversations, and keep a copy of electronic communications, that relate to the activities (investments and fund management including alternative investment fund management) around *financial instruments*

Provided by the *firm* to an *employee* or contractor; or

1. The use of which by an *employee* or contractor has been accepted or permitted by the *firm*.

A *firm* must take all reasonable steps to prevent an *employee* or contractor from making, sending, or receiving relevant telephone conversations and electronic communications on privately-owned equipment which the *firm* is unable to record or copy. The telephone conversations and electronic communications referred to include those that are intended to result in the performance of the regulated activities in *financial instruments* that the firm is authorised for, even if those conversations or communications do not in fact result in the performance of such activities.

Exemption from recording all phone conversations

Firms that do not hold client funds, or only provide investment advice and provide services solely or mainly to *retail clients* are not required to record all telephone conversations as required above subject to compliance with the following requirements:

1. A telephone conversation that would be subject to the phone recording rules must be recorded instead using a written minute or note; and
2. The minute or note must include all relevant, and at least the following, information:
    1. (a) date and time of the conversation;
    2. (b) identity of the individual participants in the conversation;
    3. (c) initiator of the conversation; and
    4. (d) relevant information about the client order, including the price, volume, type of order and when it will be transmitted or executed.

Firms that choose to take advantage of the exemption from recording all phone conversations, should set out its decision in its recording policy. Further, any minute or note made in accordance with the exemption should contain all relevant substantive details of the conversation, as well as the information to be written in notes or minutes as set out above. All such notes or minutes should be

stored in a durable medium which allows them to be replayed or copied; and retained in a format that does not allow the original record to be altered or deleted.

A *firm* must notify new and existing *clients* that telephone communications or conversations between the *firm* and its *clients* that result or may result in activities in *financial instruments* referred to above which are not sold over the counter - or offered for public placements. The notification must be made before the provision of any *investment services* to new and existing *clients*. These notifications should be made to the following.

1. To a new *client* prior to the provision of any *investment services*; and
2. To an existing *client* prior to the provision of any *investment services* following:
    1. (a) the commencement of these *rules*; or
    2. (b) the *firm* otherwise becoming subject to these *rules*, after the date of commencement.

Obligation for other communications

Client instructions given otherwise than by telephone must be made in a *durable medium* such as by mail, faxes, emails or documentation of *client* instructions issued at meetings. In particular, the content of relevant face-to-face conversations with a *client* may be recorded by using written minutes or notes.

Record keeping - SYSC 10A.1.14

The records kept in accordance with this chapter must be:

1. Provided by the *firm* to the *client* involved upon request; and
2. Kept for a period of five years and, where requested by the *FCA*, for a period of up to seven years.

Group risks / Financial conglomerates

The purpose of this chapter of the hand book is to set out how the systems and control requirements imposed by *SYSC* apply where a *firm* is part of a *group*. If a *firm* is a member of a *group*, it should be able to assess the potential impact of risks arising from other parts of its *group* as well as from its own activities.

General rule - SYSC 12.1.8

A *firm* must:

1. (1) have adequate, sound and appropriate risk management processes and internal control mechanisms for the purpose of assessing and managing its own exposure to *group* risk, including sound administrative and accounting procedures; and
2. (2) ensure that its *group* has adequate, sound and appropriate risk management processes and internal control mechanisms at the level of the *group*, including sound administrative and accounting procedures.

This means that the question of whether the risk management processes and internal control mechanisms are adequate, sound and appropriate should be judged in the light of the nature, scale and complexity of the *group's* business and of the risks that the *group* bears. Risk management processes must also include the stress testing and scenario analysis required by the *PRA* Rulebook.

This includes internal control mechanisms that are adequate for the purpose of producing any data and information which would be relevant for the purpose of monitoring compliance with any prudential requirements (including any reporting requirements and any requirements relating to capital adequacy, solvency, systems and controls and large exposures

Financial conglomerates - SYSC 12.1.11

The FCA expects the following from financial conglomerates.

1. Sound governance and management processes, which must include the approval and periodic review by the appropriate managing bodies within the *financial conglomerate* of the strategies and policies of the *financial conglomerate* in respect of all the risks assumed by the *financial conglomerate*, such review and approval being carried out at the level of the *financial conglomerate*;
2. Adequate capital adequacy policies at the level of the *financial conglomerate*, one of the purposes of which must be to anticipate the impact of the business strategy of the *financial conglomerate* on its risk profile and on the capital adequacy requirements to which it and its members are subject;
3. Adequate procedures for the purpose of ensuring that the risk monitoring systems of the *financial conglomerate* and its members are well integrated into their organisation;
4. Adequate procedures for the purpose of ensuring that the systems and controls of the members of the *financial conglomerate* are consistent and that the risks can be measured, monitored and controlled at the level of the *financial conglomerate*; and
5. Arrangements in place to contribute to and develop, if required, adequate recovery and resolution arrangements and plans; a *firm* must update these arrangements regularly.

Where this section applies with respect to a *financial conglomerate*, the internal control mechanisms referred to above or, for a *Solvency II firm*, the internal control system referred to in the PRA Rulebook: Solvency II firms: Conditions Governing Business, rule 3, must include:

1. Mechanisms that are adequate to identify and measure all material risks incurred by members of the *financial conglomerate* and appropriately relate capital in the *financial conglomerate* to risks; and
2. Sound reporting and accounting procedures for the purpose of identifying, measuring, monitoring and controlling *intra-group transactions* and *risk concentrations*.

Employee responsibilities

A *firm* should ensure that all *employees* are capable of performing, and aware of, their operational risk management responsibilities, including by establishing and maintaining:

1. Appropriate segregation of *employees*' duties and appropriate supervision of *employees* in the performance of their responsibilities
2. Appropriate recruitment and subsequent processes to review the fitness and propriety of *employees*
3. Clear policy statements and appropriate systems and procedures manuals that are effectively communicated to *employees* and available for *employees* to refer to as required. These should cover, for example, compliance, IT security and health and safety issues;
4. Training processes that enable *employees* to attain and maintain appropriate competence; and
5. Appropriate and properly enforced disciplinary and employment termination policies and procedures.

Operational risks - SYSC 13.7 Processes and Systems

A firm should establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others). In doing so a firm should have regard to:

(1) the importance and complexity of processes and systems used in the end-to-end operating cycle for products and activities (for example, the level of integration of systems);

(2) controls that will help it to prevent system and process failures or identify them to permit prompt rectification (including pre-approval or reconciliation processes);

(3) whether the design and use of its processes and systems allow it to comply adequately with regulatory and other requirements;

(4) its arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and

(5) the importance of monitoring indicators of process or system risk (including reconciliation exceptions, compensation payments for client losses and documentation errors) and experience of operational losses and exposures.

Internal documentation may enhance understanding and aid continuity of operations, so a firm should ensure the adequacy of its internal documentation of processes and systems (including how documentation is developed, maintained and distributed) in managing operational risk. A firm may use external documentation (including contracts, transaction statements or advertising brochures) to define or clarify terms and conditions for its products or activities, its business strategy (for example, including through press statements), or its brand. Inappropriate or inaccurate information in external documents can lead to significant operational exposure.

A firm should ensure the adequacy of its processes and systems to review external documentation prior to issue (including review by its compliance, legal and marketing departments or by appropriately qualified external advisers). In doing so, a firm should have regard to:

(1) compliance with applicable regulatory and other requirements;

(2) the extent to which its documentation uses standard terms (that are widely recognised, and have been tested in the courts) or non-standard terms (whose meaning may not yet be settled or whose effectiveness may be uncertain);

(3) the manner in which its documentation is issued; and

(4) the extent to which confirmation of acceptance is required (including by customer signature or counterparty confirmation).

IT systems - SYSC 13.7.5

IT systems include the computer systems and infrastructure required for the automation of processes, such as application and operating system software; network infrastructure; and desktop,

server, and mainframe hardware. Automation may reduce a firm's exposure to some 'people risks' (including by reducing human errors or controlling access rights to enable segregation of duties), but will increase its dependency on the reliability of its IT systems. A firm should establish and maintain appropriate systems and controls for the management of its IT system risks, having regard to:

(1) its organisation and reporting structure for technology operations (including the adequacy of senior management oversight);

(2) the extent to which technology requirements are addressed in its business strategy;

(3) the appropriateness of its systems acquisition, development and maintenance activities (including the allocation of responsibilities between IT development and operational areas, processes for embedding security requirements into systems); and

(4) the appropriateness of its activities supporting the operation of IT systems (including the allocation of responsibilities between business and technology areas).

Failures in processing information (whether physical, electronic or known by employees but not recorded) or of the security of the systems that maintain it can lead to significant operational losses. A firm should establish and maintain appropriate systems and controls to manage its information security risks. In doing so, a firm should have regard to:

(1) confidentiality: information should be accessible only to persons or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;

(2) integrity: safeguarding the accuracy and completeness of information and its processing;

(3) availability and authentication: ensuring that appropriately authorised persons or systems have access to the information when required and that their identity is verified;

(4) non-repudiation and accountability: ensuring that the person or system that processed the information cannot deny their actions.

A firm should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799 (Information Security Management).

Geographic location and operational risk

Operating processes and systems at separate geographic locations may alter a firm's operational risk profile (including by allowing alternative sites for the continuity of operations). A firm should understand the effect of any differences in processes and systems at each of its locations, particularly if they are in different countries, having regard to:

(1) the business operating environment of each country (for example, the likelihood and impact of political disruptions or cultural differences on the provision of services);

(2) relevant local regulatory and other requirements regarding data protection and transfer;

(3) the extent to which local regulatory and other requirements may restrict its ability to meet regulatory obligations in the United Kingdom (for example, access to information by the FCA and local restrictions on internal or external audit); and

(4) the timeliness of information flows to and from its headquarters and whether the level of delegated authority and the risk management structures of the overseas operation are compatible with the firm's head office arrangements.

SYSC 18.3 Internal arrangements - Whistleblowing

A firm must establish, implement and maintain appropriate and effective arrangements for the disclosure of reportable concerns by whistleblowers.

The internal arrangements must at least:

1. (a) be able effectively to handle disclosures of *reportable concerns* including:
    1. (i) where the *whistleblower* has requested confidentiality or has chosen not to reveal their identity; and
    2. (ii) allowing for disclosures to be made through a range of communication methods;
2. (b) ensure the effective assessment and escalation of *reportable concerns* by *whistleblowers* where appropriate, including to the *FCA* or *PRA*;
3. (c) include reasonable measures to ensure that if a *reportable concern* is made by a *whistleblower* no *person* under the control of the *firm* engages in victimisation of that *whistleblower*;
4. (d) provide feedback to a *whistleblower* about a *reportable concern* made to the *firm* by that *whistleblower*, where this is feasible and appropriate;
5. (e) include the preparation and maintenance of:
    1. (i) appropriate records of *reportable concerns* made by *whistleblowers* and the *firm's* treatment of these reports including the outcome; and
    2. (ii) up-to-date written procedures that are readily available to the *firm's UK-based employees* outlining the *firm's* processes for complying with this chapter;
6. (f) include the preparation of the following reports:
    1. (i) a report made at least annually to the *firm's governing body* on the operation and effectiveness of its systems and controls in relation to whistleblowing (see *SYSC 18.3.1R*); this report must maintain the confidentiality of individual whistleblowers; and
    2. (ii) prompt reports to the *FCA* about each case the *firm* contested but lost before an employment tribunal where the claimant successfully based all or part of their claim on either detriment suffered as a result of making a protected disclosure in breach of *section 47B* of the Employment Rights Act 1996 or being unfairly dismissed under *section 103A* of the Employment Rights Act 1996;

7. (g) include appropriate training for:
    1. (i) *UK*-based *employees*;
    2. (ii) *managers* of *UK*-based *employees* wherever the *manager* is based; and
    3. (iii) *employees* responsible for operating the *firms'* internal arrangements.

How to establish whistleblowing arrangements

When establishing internal arrangements in line with SYSC 18.3.1R a firm may:

1. (a) draw upon relevant resources prepared by whistleblowing charities or other recognised standards setting organisations; and
2. (b) consult with its *UK*-based *employees* or those representing these *employees*.

In considering if a *firm* has complied with *SYSC 18.3.1R* the *FCA* will take into account whether the *firm* has applied the measures in (1).

A *firm* may wish to clarify in its written procedures for the purposes of *SYSC 18.3.1R(2)(e)(ii)*, that: (a) there may be other appropriate routes for some issues, such as employee grievances or consumer complaints, but internal arrangements as set out in *SYSC 18.3.1R(2)* can be used to blow the whistle after alternative routes have been exhausted, in relation to the effectiveness or efficiency of the routes; and (b) nothing prevents *firms* taking action against those who have made false and malicious disclosures.

1. A *firm* may wish to operate its arrangements under *SYSC 18.3.1R* internally, within its *group* or through a third party.

2. *Firms* will have to consider how to manage any conflicts of interest.
3. If the *firm* uses another member of its group or a third party to operate its arrangements under *SYSC 18.3.1R* it will continue to be responsible for complying with that *rule*.

Whistleblowing - Training and development

A firm's training and development in should include: for all UK-based employees:

1. (a) a statement that the firm takes the making of reportable concerns seriously;
2. (b) a reference to the ability to report reportable concerns to the firm and the methods for doing so;
3. (c) examples of events that might prompt the making of a reportable concern;
4. (d) examples of action that might be taken by the firm after receiving a reportable concern by a whistleblower, including measures to protect the whistleblower's confidentiality; and
5. (e) information about sources of external support such as whistleblowing charities;

For all managers of UK-based employees wherever the manager is based:

6. (a) how to recognise when there has been a disclosure of a reportable concern by a whistleblower;
7. (b) how to protect whistleblowers and ensure their confidentiality is preserved;
8. (c) how to provide feedback to a whistleblower, where appropriate;
9. (d) steps to ensure fair treatment of any person accused of wrongdoing by a whistleblower; and
10. (e) sources of internal and external advice and support on the matters referred to above.

A whistleblower's confidentiality should be protected.

Reporting of concerns by employees to regulators

Firms must ensure that their *appointed representatives* or, where applicable, their *tied agents*, inform any of their *UK*-based *employees* who are *workers* that, as *workers*, they may make *protected disclosures* to the *FCA*.

Appointed representatives and tied agents

Firms are encouraged to invite their appointed representatives or, where applicable, their tied agents to consider adopting appropriate internal procedures which will encourage workerswith concerns to blow the whistle internally about matters which are relevant to the functions of the FCA or PRA.

Link to fitness and propriety

The FCA would regard as a serious matter any evidence that a firm had acted to the detriment of a whistleblower. Such evidence could call into question the fitness and propriety of the firm or relevant members of its staff, and could therefore, if relevant, affect the firm's continuing satisfaction of threshold condition 5 (Suitability) or, for an approved person or a certification employee, their status as such.
