Version: April 2014

SENIOR MANAGEMENT ARRANGEMENTS, SYSTEMS AND CONTROLS (SYSC)

2. Senior Management Arrangements, Systems and Controls (SYSC)

From 1 April 2009 the "common platform" rules applied to all firms other than insurers, managing agents and the Society of Lloyd's. These firms remain subject to SYSC 2 and 3. All other firms are no longer subject to SYSC 2 and 3 but to SYSC 4 to 10.

General insurance firms are subject to detailed rules and guidance on systems and controls, however much of the content is to be considered guidance rather than rules. The FCA has however stated that it should be applied in a "proportionate manner, taking into account the nature, scale and complexity of the firm's business".

A table summarising the requirements including whether they should be treated as rules or guidance, is included in the template section at the end of this chapter (SYSC Template 13).

This sourcebook promotes Principle 3, "a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems".

Responsibility for compliance is on a top-down basis and the FCA are quite clearly giving responsibility for the organisation of the firm and its compliance with regulations to the senior managers. The senior managers need to recognise and understand their responsibilities and these need to be confirmed on a formal written basis.

This sourcebook looks at the way the firm organises itself and the way it splits its responsibilities amongst its senior management.

The main purposes of SYSC are to:

- Encourage Directors and Senior Managers to take responsibility for the firm's arrangements on matters likely to be of interest to the FCA.

- Ensure that firms are clear on how they need to organise and control their affairs responsibly and effectively, with adequate risk management systems.

- Encourage firms to allocate responsibility for effective and responsible organisation to specific directors and senior managers.

The systems and controls of the firm need to operate in a way that help it to comply with its regulatory obligation. Systems and Controls need to be established and maintained in the following areas:

- governance and organisational structure;
- monitoring of systems and controls;
- compliance;
- risk assessment;
- management information;
- skills knowledge and expertise;
- audit committee;
- internal audit;
- outsourcing;
- conflicts of interest;
- business continuity; and
- records.

The FCA would expect the firm to have considered the following issues in establishing and maintaining their systems and controls:

- the size of the firm;
- the scale and complexity of the business (small firms are not expected to have the full range of procedures and systems that a well run large firm requires);
- the need to counter the risk that the firm might be used to further financial crime (see section 2.10 on Proceeds of Crime Act 2002);
- the diversity of operations; and
- the volume and size of transactions.

Financial crime is defined as any offence involving fraud, dishonesty, misconduct in or misuse of, information relating to any financial market or handling directly or indirectly the proceeds of crime.

It is important however that whatever the size of the firm it should be able to demonstrate that it has considered which systems and controls are relevant to its business.

A firm should establish, implement and maintain adequate internal controls designed to secure compliance with decisions and procedures at all levels of the firm.

As well as clear documentation of procedures, firms need to ensure that they can clearly evidence how procedures have been complied with throughout the organisation. It is vitally important therefore that **such information should be kept both up to date and communicated to all members of staff.**

2.1 General Requirements

2.1.1 Governance

The supervision of business activities is the responsibility of the management of the organisation. A firm must have robust governance arrangements which include:

- clear organisational structure;
- clear lines of responsibility;
- effective risk management processes which identify, manage, monitor and report risks that the business may be exposed to;
- effective internal controls including administrative and accounting procedures; and
- effective controls and safeguards for IT systems.

These arrangements and controls should be comprehensive but proportionate to the size, nature and complexity of the business and should take into account any technical criteria required by the firm's business continuity planning.

Firms should ensure that they have:

- decision making procedures and a documented organisational structure which clearly specifies reporting lines and allocates functions and responsibilities;
- adequate internal controls to ensure compliance with decisions and procedures at all levels in the firm; and
- effective internal reporting and communication of information at all levels in the firm.

Organisation charts should be produced. These should:

- clearly identify roles, authority levels, supervisory, and reporting lines for the firm;
- be communicated to all members of staff; and
- be regularly reviewed and updated.

Sample organisation charts and authority lists are included in the templates section at the end of this chapter (SYSC templates 1 to 3).

Firms may wish to delegate authority to senior members of staff. Such staff will need to:

- be assessed for their suitability to perform the role;
- be able to demonstrate their competence to perform the role;
- have clearly defined and communicated limits and extents of authority; and
- be supervised and monitored, including a process for following up any actions identified if delegation is found to have fallen down.

This information should be clearly recorded and updated regularly. If firms decide to outsource any work then the same rules will apply.

As far as possible the organisation of the work should be segregated to reduce the likelihood of mismanagement and fraud.

2.1.2 Business continuity

Firms should take reasonable steps to ensure the continuity of their regulated business activities. This includes having an adequate business continuity plan in place.

What is a business continuity plan?

These are sometimes known as disaster recovery plans. They are plans that ensure that the firm can continue to function and meet their regulatory obligations in the event of unforeseen interruptions to systems and procedures e.g. fire, flood, loss of capital, loss of key staff. You should establish, implement and maintain an adequate business continuity policy.

The aim of this policy is to ensure that in the case of an interruption, any losses are limited and that essential data, functions and maintenance of regulatory activities is preserved. Where this is not possible the policy should ensure timely recovery of data, functions and resumption of regulatory activities.

What needs to be reviewed?

- How you will communicate to members of staff and to customers?
- Have you alternative office premises?
- What are your critical functions and business processes?
- Are computer files backed up and kept off site?
- How paper files are stored and is there information on them that cannot be accessed via computer?
- Do you operate a clear desk policy?
- How do you store financial accounts, cheque books etc.?
- Are your business strategy plans secure?

The firm then needs to establish and maintain an effective business continuity plan for its entire operation.

Business continuity planning

This plan should, dependent on size of the firm, but could include the following:

1. Resource requirements such as people, systems and other assets and the arrangements for obtaining these resources.
2. Documented process for implementing the business continuity plan.
3. Recovery priorities.
4. Communication arrangements for internal and external concerned parties including: FCA, clients, staff and suppliers.
5. Processes for validating the integrity of any information affected by the interruption.
6. Recovery team activities checklist.
7. Recovery team contact details.
8. Staff contact details.
9. Alternative accommodation requirements.
10. Critical business functions.
11. Critical business documents/data.
12. Critical PC/other systems applications.
13. Client list.
14. Renewal list.
15. Critical suppliers/services/markets.
16. Counselling.

The plan needs to be documented, communicated to everyone in the firm, regularly updated and tested to ensure that it actually works.

A copy of a business continuity plan is included in the template section at the end of this chapter (SYSC Template 11).

2.1.3 Regular monitoring

Firms should monitor and on a regular basis evaluate the adequacy and effectiveness of their systems and controls. To enable you to do this an audit checklist is included in the template section at the end of this chapter (SYSC Template 9). A compliance activity log detailing common compliance activities that need to be carried out during the year is also included in this section (SYSC Template 6).

2.1.4 Audit committee

Depending on the size, nature and complexity of the firm it may be appropriate to set up an audit committee. An audit committee could:

- examine management's process for ensuring the appropriateness and effectiveness of its systems and controls;
- examine the arrangements made by management to ensure compliance with requirements and standards;
- oversee the internal audit function; and
- provide an interface between management and external auditors.

An audit function should have an appropriate number of non-executive directors and formal terms of reference.

2.1.5 Persons directing the business

The senior personnel (normally Directors or equivalent) of a firm should be of sufficiently good repute and sufficiently experienced to ensure sound and prudent management of the firm.

2.1.6 Responsibility of senior personnel

A firm must ensure that directors and senior managers (senior management) have the responsibility for ensuring that the firm complies with its obligations under the regulatory system.

Senior management should receive on a regular basis, and at least annually written reports on compliance of the firm. This should include their regulatory responsibilities and risk assessments. These reports should identify the remedial action taken where deficiencies have occurred.

They must also periodically review the effectiveness of the internal procedures put in place to meet regulatory requirements and take appropriate measures to address any deficiencies.

2.1.7 Apportionment of responsibilities

This section only applies to firms who do not have an approved person with one of the governing controlled functions (CF1 to CF6).

The FCA requires a firm to apportion significant responsibilities amongst its directors, senior managers or partners, so that it is clear:

- who has responsibility; and
- that the business affairs are adequately monitored and controlled.

The firm also needs to make and keep a record of these arrangements (e.g. by means of an organisation chart). These records need to be kept up to date and kept for 6 years from the date it was superseded by a newer version.

Overall responsibility falls on the firm's chief executive, senior partner or whoever assumes executive control. If this role is shared then the responsibilities become jointly owned. If there is no chief executive or equivalent then the responsibilities will fall on the individual managers and directors responsible for the management of the firm.

With a smaller firm the business owner will become responsible for all or many of the functions.

The senior managers of the firm should be of sufficiently good repute and sufficiently experienced so as to ensure sound and prudent management of the firm.

If a firm has other approved persons with governing functions, i.e. Controlled Functions 1 to 6, they do not need to allocate CF8 (Apportionment & Oversight) specifically to one of them. CF8 is the overall responsibility for the apportionment of responsibilities and overseeing the establishment and maintenance of systems and controls and compliance with the requirements of the Insurance Conduct of Business (ICOBS) rules.

However if the firm does not have any approved persons with governing functions (likely to be very small firms or firms who are secondary intermediaries), then they will still need to allocate CF8 to at least one individual.

2.2 Skills, knowledge and expertise

A firm must employ staff with the skills, knowledge and expertise necessary for them to fulfil their role within the firm. Further guidance on ways a firm can demonstrate compliance with these rules and additional requirements for firms advising consumers can be found in Section 3, Business Standards, Chapter 4, Training and Competence.

A firm needs to have systems and controls in place to satisfy itself of the suitability of anyone acting for them. This should include their competence and honesty. This information needs to be verified:

- at recruitment; and
- in regular assessments throughout the year. It is recommended that a firm assess continued competence at least twice a year.

An individual's honesty should not need to be reviewed after recruitment unless something happens to deem this necessary.

Assessment of an individual's suitability should take into account the level of responsibility the individual will assume in the firm.

Recruitment

The skills, knowledge, experience, qualifications and employment record of a prospective employee or agent should be verified before an offer of employment or the completion of an agency agreement. Records must be retained on the personnel file of the person concerned, if employed, or on a central register and file of all agents.

Interview – a written record of the interview should be retained in the personnel file of the person concerned. This interview should be used to verify honesty and competence to perform the role. Guidance notes are set out in Section 3, Business Standards, Chapter 4, Training and Competence, template section (TC Template 1).

References - 2 written references should be obtained, unless personally known by the company. Criminal records and credit history should be obtained.

Maintenance of competence

The firm will need to demonstrate that their members of staff have maintained competence. It is recommended that staff are assessed regularly, at least every 6 months. This can be done by various means:

- interview;
- assessment test – written or oral;
- spot check of files and outgoing mail;
- workplace assessment e.g. sitting with the member of staff and observing their performance;
- role play; or
- a combination of all the above.

An example of a workplace assessment checklist can be found in the Training and Competence chapter, template section (TC Template 3).

Further rules and guidance relating specifically to firms dealing with consumers can be found in the Training and Competence section of this manual.

2.2.1 Segregation of functions

A firm should ensure that functions within the firm are segregated to prevent conflicts of interest occurring.

Effective segregation of duties is an important element in the internal controls of a firm in the prudential context. It should help ensure that no one individual is completely free to commit a firm's assets or incur liabilities on its behalf. It can also help ensure that a firm's governing body receives objective information on financial performance, risks faced by the firm and the adequacy of its systems and controls.

A firm should normally ensure that no single individual has unrestricted access to do all of the following:

- initiate a transaction;
- bind the firm;
- make payments; and
- account for it.

In some cases it may not be possible to fully segregate all duties (for example because of a limited number of staff). In this instance the firm should ensure that it has adequate controls in place to mitigate any risks imposed such as frequent reviews by a senior manager. You should on a regular basis review the adequacy and effectiveness of these controls.

2.2.2 Awareness of procedures

A firm should ensure that all relevant staff are aware and trained in the processes and procedures that must be followed to enable them to perform their role and responsibilities.

2.3 Compliance

A firm must establish, implement and maintain adequate policies and procedures to ensure that the firm complies with its regulatory responsibilities. These processes should ensure compliance at all levels of the firm including: managers, employees and appointed representatives.

The firm should maintain a permanent and effective compliance function/role (this may however just be one person with responsibility for compliance monitoring). This function/role should:

- be responsible for monitoring the firm's compliance;
- assess the adequacy and effectiveness of processes and procedures; and
- advise and assist managers, employees and appointed representatives who are responsible for carrying out any regulated activity.

This function or person should ensure that:

- all employees are trained and understand what they should do, how they should do it and when it needs to be completed by;
- procedures should be documented and available to all members of staff; and
- compliance should be monitored and any breaches need to be:
    - reported;
    - investigated to identify root cause; and
    - actions put in place to rectify the situation and also to ensure that it will not happen again.

Samples of a compliance breach report and compliance log are included in the template section end of this chapter (SYSC Templates 4 and 5). Also included in this section (SYSC Template 6) is a "Compliance activity log" which details common compliance activities that need to be carried out during the year and a Compliance Monitoring Programme (SYSC Template 6a) which outlines the monitoring that a firm should be undertaking.

It may be appropriate for a firm to have a separate compliance function. If they do then they should ensure that:

- organisation and responsibilities are documented;
- it is staffed by an appropriate number of competent staff who have the necessary expertise, authority and access to all relevant material to enable them to undertake their role;
- compliance staff are not involved in the performance of the services which they are monitoring;
- a compliance officer is appointed with responsibility for the compliance function and producing the necessary reports to the governing body;
- the method of remunerating the compliance staff must not compromise their objectivity; and
- it is adequately resourced.

2.3.1 Internal audit

Dependent on the size, nature and complexity of the organisation it may be necessary to arrange and establish an internal audit function, which is separate and independent from the other functions of the firm. This function would have the following responsibilities:

- establish, implement and maintain an audit plan to evaluate the firm's adequacy and effectiveness of their systems and controls;
- issue recommendations based on the result of any audits undertaken;
- verify compliance with those recommendations; and
- produce the annual compliance report to the governing body.

An audit checklist is included in the template section at the end of this chapter (SYSC Template 9). A compliance activity log detailing common compliance activities that need to be carried out during the year is also included in this section (SYSC Template 6).

2.4 Risk management

The FCA requires that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. This should include effective procedures for risk assessment and setting the level of risk tolerated by the firm. The responsibility for this function belongs at director, senior management or partner level.

What does this mean? The FCA want firms to identify the risks that are present in the business and implement actions to mitigate these risks.

What is a risk?

Risk is the possibility of:

- loss;
- injury;
- disadvantage;
- destruction;
- danger;
- disaster;
- a person or thing considered as a potential hazard; and
- an unforeseen event.

Risk stands between you and the fulfilment of your business objectives. To succeed you will need to identify, evaluate and overcome risk in all its guises. Some examples of risks to your business may be:

Example 1

You have a large corporate client that currently represents 40% of your annual income from general insurance activities. This client's policies are coming up for renewal.

There have been a few issues in the last year and there is a risk that this client may take his business to one of your competitors, thus reducing your revenue considerably.

Example 2

You outsource your IT to a third party software house. If there was a disaster in the software house you could lose your systems. This could impact your ability to continue to operate until systems are back on line.

Example 3

Your Compliance Officer is near to retirement and has often mentioned how he would like to retire early and live abroad. There is a risk that, if he has the opportunity to, he will leave to fulfil his dream.

Example 4

You rely on one insurer for the majority of your insurance placement. There is a risk that they could go into liquidation leaving you with no access to the insurance market. This would impact your ability to arrange insurance cover for your clients.

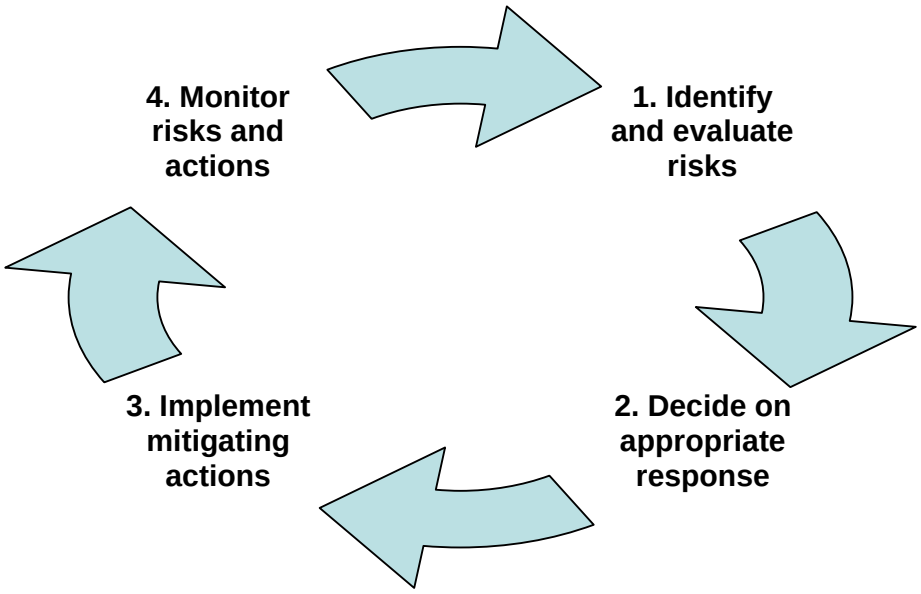
What is risk management?

Risk management is a process which allows you to reduce the impact that risks may have on your business.

A risk management system should be in place that will allow you to identify, monitor and take action on risks to the business. The FCA also require that the risk management process is responsive and proactive to enable changes to be made to a system or process if an issue presents itself.

The governing body should approve and review any risk management strategy and processes that you have in place.

The risk management process is a continual cycle as illustrated below:



1. Identify and evaluate risks e.g. risk assessment

Four easy steps to risk assessment

1. What could go wrong?
2. What would be the impact?
    a. financial;
    b. strategic;
    c. operational.
    Use a simple 1 to 5 definition (1 very low impact, 5 very high impact).
3. What is the likelihood of it happening?
    Again, use a simple 1 to 5 definition (1 very unlikely, 5 very likely).
4. Overall risk assessment is impact x likelihood.

The higher the overall score the greater the risk to the firm.

2. Decide on appropriate response

Once you have assessed the risk you need to decide how you will respond. If the overall assessment of the risk is very low (e.g. likelihood of happening = 1, impact = 1, therefore overall assessment = 1), then you may decide to do nothing but continue to monitor.

If the likelihood or impact changes then you may wish to put in place mitigating actions.

If you have assessed a risk as very high (e.g. impact 5 and likelihood 5 therefore an overall value of 25) then you will probably need to put in place immediate actions to either eliminate the risk or mitigate the impact.

3. Implement mitigating actions

In example 2 above where you outsource IT to a software house and there may be a disaster, then if this has a high impact and high likelihood then you will need to put in place some actions. These could include:

i) ensuring service level agreements are in place for the continuity of systems;
ii) ensuring that the software house has a disaster recovery plan in place and that this meets your needs;
iii) reviewing alternative methods for dealing with the IT function.

In example 3 the actions you may take are:

i) succession planning – training someone who can take over from the Compliance Officer;
ii) reviewing recruitment policies to ensure you can get someone in quickly;
iii) taking out key person insurance;
iv) talking to the individual and continuing to discuss the possibility of them leaving in periodic reviews.

4. Monitor risks and actions

You should continually monitor your existing risks and actions to ensure that they are having the desired effect and to ensure that nothing has changed. You should also continually be identifying and evaluating all risks for the business. As the business changes new risks will appear and existing risks may disappear.

Sample regulatory risk log and risk assessment forms are included in the template section at the end of this chapter (SYSC Templates 7 and 8).

Key Person Risk

The loss of a key person can often be a major concern to smaller businesses, as these people tend to hold vital information or knowledge of the business or its processes.

However there are some easy steps that a firm can take to mitigate this risk including:

- training (so that the skills or knowledge of the key person can be spread more widely);
- storing copies of key documents at more than one location;
- encouraging key people to share their control and influence by introducing revolving roles or work shadowing; and
- regular testing of staff on their understanding of key areas of the business.

How to reduce risk in smaller firms

Keeping important documents can assist firms in reducing risks. These could include:

- board minutes;
- business contingency plans;
- business plans, action logs and risk maps;
- strengths, weaknesses, opportunities and threats analysis; and
- comprehensive office manuals – giving step by step instructions on how, when and by whom each task is completed.

2.5 Outsourcing

A firm may outsource activities to a third party, however it cannot outsource or delegate its regulatory responsibilities. When relying on a third party for performance of operational functions which are critical for the performance of a regulated activity then the firm should ensure:

- it takes reasonable steps to avoid any additional operational risk;
- it does not impair materially the FCA's ability to monitor the firms compliance with FCA regulation;
- it has effective processes to identify, manage, monitor and report risks;
- has adequate and effective internal controls in place;
- it has informed the FCA that it intends to outsource the function to a third party; and
- makes available to the FCA on request all information necessary for the FCA to supervise compliance of the outsourced activities.

If a firm outsource critical operational functions or services, it remains fully responsible for discharging all of its regulatory obligations and must comply with the following conditions:

- the outsourcing must not result in the delegation by senior management of their responsibility;
- the relationship and obligations of the firm towards its clients under the regulatory system must not be altered;
- the conditions with which the firm must comply to be authorised must not be undermined; and
- none of the conditions for the firm's authorisation must be removed or modified.

The firm should have a written agreement in place with all third parties performing outsource functions identifying its own responsibilities, third party responsibilities, activities that are to be outsourced and the means for terminating the contract.

Activities that are not deemed critical include:

- provision of advisory services and other services which do not form part of the relevant services of the firm such as: legal advice, staff training, billing services and security of the firm's premises and staff; and
- purchase of standardised services such as market information services and provision of price feeds.

Outsourcing activities to service providers

A firm should, before outsourcing an activity, ensure the following conditions are met:

- the service provider has the ability, capacity and authorisation;
- the service provider can carry out the service effectively (the firm will need to be able to assess this effectively) and that action is taken if this does not happen
- the service provider can adequately supervise the operation of the function or service;
- the firm has adequate expertise and resource to monitor the service provider;
- the service provider must disclose to the firm any development which may materially impact its ability to continue to undertake the outsourced activity;
- the firm is able to terminate the arrangement without detriment to the continuity and quality of the provision of the service;
- the service provider must co-operate with the FCA;
- the firm, its auditors and the FCA must have affective access to data related to outsource activity, as well as the business premises of the service provider;
- the service provider must protect any confidential information relating to the firm and its clients;
- the firms and service provider must maintain a business continuity plan and undertake periodic testing if back up facilities; and
- there must be a written agreement in place detailing the respective rights and obligations of the firm and the service provider (we would recommend that firms obtain an independent review of any outsourcing agreements before entering into any outsourcing arrangements).

2.6 Record keeping

A firm must arrange for orderly records to be kept of their business and internal organisation, including all services and transactions. This must be sufficient to allow the FCA to monitor the firm's compliance with regulatory requirements. These records should be capable of being reproduced in English (if required or appropriate).

The general principle is these records should be kept for as long as it is relevant for the purpose for which they are made. However for certain records the FCA may require them to be kept for either 3 years or 6 years.

Appropriate records need to be kept in the following areas:

1. Senior Management Arrangements.
2. Compliance with regulation.
3. Sales and administration.
4. Training and competence
5. Appointed representatives.
6. Accounting and auditors' reports.
7. Complaints.
8. Systems and Controls.

Senior Management Arrangements (SYSC)

A record of the arrangements of the organisation must be kept. This includes apportionment and oversight and the split of responsibilities. This can be by means of organisational charts, job descriptions, project management documents and terms of references.

These records need to be regularly updated and need to be kept for 6 years.

Compliance with regulation

You will need to keep records of any audits that are performed and any compliance breaches that are found. You should record all compliance breaches, the action taken to rectify the situation and the action taken to stop it happening again.

Significant breaches may need to be reported to the FCA. It is recommended that significant breaches are kept for 6 years in line with the auditor report requirements.

Sales and administration (ICOBS)

The FCA have not specifically identified records they wish firms to keep. Firms should however bear in mind that to deal with requests of information from the FCA and their own customers they may require evidence of matter such as:

- the reasons for a personal recommendation
- documentation provided to a customer
- how claims have been settled and why

Training and Competence – sales staff/approved persons

A firm must make appropriate records to demonstrate compliance with the rules in this sourcebook and keep them for 3 years following periods after an employee stops carrying on the activity. Suggested records to comply with this rule would include:

1. Recruitment – record the process followed to recruit the person including how you determined they were suitable e.g. application form, interview notes, credit and criminal record checks etc.
2. Information on how you assess training needs of staff and how you then meet these training needs.
3. Assessing competence – the criteria used to assess whether someone has attained competence and when they attained competence.
4. Maintaining competence – the criteria used to assess continued competence (e.g. written assessments and practical assessments) and whether the employee has in fact maintained competence. If they have not, what actions have been put in place to rectify this?
5. Supervision and monitoring – the criteria used to assess the supervision and monitoring of both staff that are not yet competent and those that are competent. How the monitoring and supervision of staff will be carried out.

Appointed representative (AR)

The following records need to be kept on the AR for 3 years following termination or amendment of an AR contract:

a. the AR's name;
b. a copy of the original contract with the AR and any subsequent amendments to it including any restrictions placed on activities;
c. the date and reason for terminating or amending a contract with an AR; and
d. any agreements with other Principals.

The firm will also need to be satisfied that the AR keeps appropriate records.

Accounting and auditor records

1. Client money – retain sufficient records to show and explain the firm's transactions and commitments. These need to be kept current and up to date and will need to be kept for 3 years after the record is made. (CASS 5.5.84R)
2. Client money shortfall – record each client's entitlement to client money shortfall. Up to date records need to be kept until the client is repaid.
3. Financial accounts for 6 years.
4. Auditor reports for 6 years. Auditors will need to produce a client asset report which includes the following:
    a. the firm has maintained systems adequate to enable it to comply with the Client Asset rules throughout the period since the last date as at which a report was made;
    b. the firm was in compliance with the rules as at the date on which the report was made;
    c. if a secondary pooling event has occurred the firm complied with rules in relation to a pooling event.
5. The auditor's report must be produced not longer than 53 weeks following the last report.

Complaints

The following information needs to be kept for a minimum of 3 years from when an eligible complaint is received:

1. the name of the complainant;
2. the substance of the complaint;
3. copies of correspondence between your firm and the complainant; and
4. details of any redress offered by your firm.

In addition the firm will need to keep records to allow them to meet FCA reporting requirements.

Other records

Records should be kept on the following:

- business strategy;
- business continuity plans;
- recruitment and personnel records;
- annual declaration on financial standing and criminal records for approved persons and retail sales advisors;
- criminal record and credit checks.

2.7 Conflicts of Interest

A firm must take all reasonable steps to identify conflicts of interest between:

- the firm, including its managers, employees, appointed representatives or any other person directly or indirectly linked to them by control and a client of the firm; and
- one client of the firm and another client.

The FCA will expect the firm to identify all potential or actual conflicts of interest and to put in place controls to manage those conflicts. These controls should include a conflicts of interest policy which is approved and regularly reviewed by the governing body of the firm and is monitored by the compliance officer of the firm (if there is one).

When identifying potential conflicts of interest the FCA will expect the firm to take into account as a minimum, whether the firm or individual involved:

- is likely to make a financial gain or avoid a financial loss at the expense of the client;
- has an interest in the outcome of the service provided of a service provided to the client which is distinct from the clients interest in that outcome;
- has a financial or other incentive to favour the interest of another client or group of clients over the interest of another client;
- carries on the same business as the client; or
- receives or will receive an inducement, other than from the client in relation to the service provided to the client.

An insurance intermediary must address actual and potential conflicts of interest arising within the firm. To do this they:

- must take reasonable care to establish and maintain systems and controls as appropriate to its business;
- maintain and operate effective organisation and administrative arrangements to ensure that reasonable steps are taken to prevent conflicts of interest arising;
- if the arrangements to manage conflicts of interest are not sufficient to ensure that the firm has confidence that it has mitigated the risk of damage to the customers' interest then the firm must clearly disclose this to the customer before undertaking the business. This disclosure must provide sufficient detail of the conflict, taking into account the nature of the client, to enable the client to make an informed decision with respect to the service in the context of which the conflict arises. Firms still need to ensure that they consider how to manage conflicts and should not over rely on disclosure;
- Firms should aim to identify and manage conflicts of interest arising in relation to both their business lines and their group activities under a comprehensive conflict of interest policy.

Further information on identifying and managing conflicts of interest including a conflicts of interest policy can be found in Special Topics chapter at the end of this manual.

2.8 Other controls

The following items are no longer specifically required under SYSC rules. However they are implicit within the rules and guidance and are considered good business practice.

2.8.1 Business strategy

One of the most significant changes in the FCA's regulatory approach is that they expect firms to be proactive in running their business and establishing a compliant regime.

What does this mean?

They will expect you to take into account the future look of the business in any planning you do today.

Examples are:

1. If the firm intends to grow through acquisition of new businesses this must be taken into account in your solvency margins and also in your systems and controls - these need to be sufficient to meet the future intentions of the business.

2. If the firm has older members of staff in key areas they expect the firm to have considered succession planning.

The FCA is not prescriptive about the form such a plan should take. However they will expect it to be documented and the achievement against such a plan to be monitored.

What should a business strategy plan include?

- company vision, aims and objectives;
- a plan as to how the company will meet its aims and objectives;
    - you may have separate plans for training, recruitment, sales generation but all should link back to the main aims and objectives; and
- for FCA purposes the business plan should identify, manage and control regulatory risk.

A copy of a business strategy plan is included in the template section at the end of this chapter (SYSC Template 10).

2.8.2 Management information

To ensure a firm is able to meet its obligations under Systems and Controls, and in particular those pertaining to monitoring compliance, risk control and conflicts of interest, a firm should provide its 'governing body' with the information it needs to play its part in identifying, measuring, managing and controlling risks of regulatory concern". Risks of regulatory concern are those risks which relate to fair treatment of customers, protection of consumers, confidence in the financial system and prevention of financial crime.

What is management information?

Management information is the data needed to ensure a firm is able to run the business on a day to day basis and also look forward to the future. It is up to you to decide what information is required, when, and for whom, so that you can organise and control your activities and can comply with your regulatory obligations.

The FCA has stressed that the detail and extent of information required will depend on the nature, scale and complexity of the business. For smaller businesses you may want to know everything that is happening in the business. However for larger businesses you may only want aggregate and summary information.

The FCA requires that a firm's management information (MI) is meeting the following criteria:

- sufficient to identify, measure and control all the material risks in the business including new products and new business;
- timely to enable prompt action to be taken where necessary;
- detailed enough (without being so detailed as to lose impact) for the various levels of management (including the 'governing body') that use it;
- covers the activities of branches, subsidiaries or appointed representatives;
- not just be about static historical data, but also considers the possible range and variability of potential outcomes. So it should:
    - include the results of stress and scenario testing to help identify the financial impact of risks in different scenarios e.g. results of any disaster recovery tests; and
    - measure the ability of the business to withstand adverse conditions over a prolonged period e.g. slump in insurance sales.

Good MI should enable management to make good decisions and to do this it needs to be:

- **Accurate** – the correct numbers with any commentary contributed by the right people;
- **Timely** – available sufficiently quickly after the relevant business activity to enable managers to act;
- **Relevant** – displaying what a manger can directly influence or something that they may need to be escalated to someone who can take the appropriate action; and
- **Consistent** – consistent on a period to period basis to allow managers to spot trends and make sound decisions.

Examples of other types of MI that a firm might produce (according to their size and spread of business) include:

- profit and loss (including a breakdown of the results) for significant business/geographic areas or product lines;
- comparison of actual spend versus budget and explanation of variances;
- risk/reward information, capital used and allocation;
- sales and losses;
- customer satisfaction measures and complaints;
- performance of service providers;
- market share data;
- compliance with regulatory requirements (financial and other) e.g. breaches and actions taken;
- information on all risks facing the business including insurance, credit, market and operational risks (for example, processing and documentation errors, claims handling, business interruption, financial crime) and legal risk;
- potential conflicts of interest; and
- staff information, such as those joining the firm, leavers, those attaining professional qualification, promotions and succession planning.

2.9 Whistle blowing

The FCA encourages firms to consider adopting (and to invite their appointed representatives to consider adopting) appropriate internal procedures which will encourage workers with concerns to blow the whistleblow internally about matters which are relevant to the FCA.

Smaller firms may choose to have less extensive procedures in place than larger firms. For example, smaller firms may not need written procedures. The following is a list of things that member firms may consider as appropriate internal procedures:

(i) telling workers that the firm takes failures seriously and explaining how wrong-doing affects the organisation;
(ii) informing workers as to what conduct is regarded as a failure;
(iii) telling workers who raise concerns that their confidentiality will be respected, if they wish this;
(iv) making it clear that workers will be supported and protected from reprisals;
(v) nominating a senior officer as an alternative route to line management and telling workers how they can contact that individual in confidence;
(vi) making it clear that false and malicious allegations will be penalised by the firm;

(vii) telling workers how they can properly blow the whistle outside the firm if necessary;
(viii) providing access to an external body for advice such as an independent charity; such as Public Concern at Work (http://www.pcaw.org.uk) on 020 7404 6609; and
(ix) encouraging managers to be open to concerns.

The FCA also requests that firms should also consider telling workers (through the firm's internal procedures, or by means of an information sheet available from the FCA's website, or by some other means) that they can blow the whistle to the FCA, as the regulator prescribed in respect of financial services and markets matters under Public Interest Disclosure Act (PIDA).

A qualifying disclosure, under PIDA, is a disclosure, made in good faith, of information which, in the reasonable belief of the worker making the disclosure, tends to show that one or more of the following (a "failure") has been, is being, or is likely to be, committed:

(i) a criminal offence; or
(ii) a failure to comply with any legal obligation; or
(iii) a miscarriage of justice; or
(iv) the putting of the health and safety of any individual in danger; or
(v) damage to the environment; or
(vi) deliberate concealment relating to any of (i) to (v).

It is immaterial whether the relevant failure occurred, occurs or would occur in the United Kingdom or elsewhere, and whether the law applying to it is that of the United Kingdom or of any other country or territory. Such disclosures may include for example:

- consistent breaches in the standards of FCA compliance;
- other agents or intermediaries acting without due authorisation after January 2005.

The FCA will give priority to live concerns or matters of recent history, and will emphasise that the worker's first port of call should ordinarily be the firm.

Firms should also note that the FCA would regard as a serious matter any evidence that a firm had acted to the detriment of a worker because he had made a protected disclosure about matters which are relevant to the functions of the FCA. 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, his status as such.

An example of a whistle blowing procedure is included in the template section at the end of this chapter (SYSC Template 12).

2.10 Financial Crime, Proceeds of Crime Act 2002, Data Security.

2.10.1 Financial Crime

Financial crimes include fraud, laundering the proceeds of crime, the finance of terrorism, bribery and corruption and the abuse of financial markets.

As well as meeting FCA requirements, firms will have wider obligations, for example, Proceeds of Crime Act 2002, Bribery Act 2010 and the Terrorism Act 2000.

How might your firm be affected?

There are number of ways that smaller businesses could be affected by Financial Crime, for example:

- A criminal using your firm's services to disguise the source of illicit funds;
- A customer defrauding your firm;
- A customer being defrauded by a third party because of your firm's actions (by, as example, unintentionally allowing the customers details to be accesses by a third party);
- Helping a customer whether intentionally or not to defraud a third party such as HM Revenue and Customs; or
- A staff member defrauding your firm.

Fraud

Fraud offences can affect both firms and individuals. There needs to be:

- Intent to make a gain or cause someone else to make a loss; and
- The existence of certain behaviours such as making a misrepresentation, failing to disclose information or misusing your position.

Examples of fraud include:

- Advising a customer to take out an insurance policy which you know is unsuitable;
- Using information supplied by a customer in your own interest rather than that of the customer;
- Misappropriation of client money or money held under risk transfer agreements;
- Failure to pass on premiums, refunds or claims;
- Falsifying customer details to obtain insurance business that would otherwise be turned down or be more expensive;
- Issuing false cover notes or false certificates of insurance;
- Individuals, whether they be clients or third parties using your firm to make false insurance claims; and
- Colluding with a customer to make false claims.

If you suspect fraud you should contact the FCA contact centre to discuss it further. You will need to supply the following information:-

- the name of the firm;
- details of any individuals involved;
- details and evidence of the suspected and/or proven fraud or financial crime;
- the names of the customers involved; and
- a summary of any investigation you have made.

What you need to do

The FCA expects firms to have risk management systems and controls in place to address the risk of financial crime. For further information on risk assessment and management please see section 2.4 above.

Firms must:

- Carry out an assessment of financial crimes risks your firm faces;
- Be able to demonstrate that risk assessment was systematic and not a ”one off” exercise; and
- Ensure that senior managers understand the identified risks and take appropriate action to mitigate them.

A financial crime checklist is included in the template section at the end of this chapter (SYSC Template 14).

2.10.2 Proceeds of Crime Act 2002

There are three primary offences under the Act and they apply to **all** insurers and intermediaries, including those involved in general insurance business.

1. Concealing (s.327)

   Where someone knows or suspects that property is a benefit from criminal conduct or it represents such a benefit (in whole or in part, directly or indirectly) then they commit an offence if they conceal, disguise, convert, transfer or remove that criminal property from England and Wales, Scotland or Northern Ireland.

2. Arranging (s.328)

   An offence is committed by a person if they enter into or become concerned in an arrangement which they know or suspect, facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

3. Acquisition, use and possession (s.329)

   An offence is committed if someone, knowing or suspecting that property is a person's benefit from criminal conduct (in whole or in part, directly or indirectly) acquires, uses or has possession of the property.

2.10.3 Reporting requirements

Although general insurance intermediaries are not subject to the Money Laundering Regulations 2003, the primary money laundering offences and tipping off offence still apply to all individuals and businesses. If a person knows or suspects that one of the above primary offences is happening and does not make a proper disclosure they will not be able to rely upon their "unregulated status" as a Defence in a Court of Law if they are charged with a primary offence.

It is therefore recommended that all firms make an authorised disclosure to the National Crime Agency which assumed responsibility for such disclosures from the Serious Organised Crime Agency in October 2013. Disclosure is made through Suspicious Activity Reports (SARs) which may be logged both manually and online.
https://www.ukciu.gov.uk/(ehng0xqshz1fbk2m2wmdw5u4)/saronline.aspx

NCA will analyse any report it receives and check it against its database for possible related information, prior to passing details on for investigation. The information is then forwarded to the Police or to Customs or another appropriate agency.

If a firm makes an authorised disclosure in relation to a suspicious transaction which has not yet been carried out, then the firm should obtain consent to proceed with the transaction from NCA. Firms should only proceed with a transaction where disclosure has been made to the NCA and:

- NCA consent has been obtained; or
- seven working days have expired without a response being received from NCA; or
- consent was refused by NCA but a 31 day period has expired without notification that law enforcement has taken further action to restrain the transaction.

The receipt of a suspicious report will be acknowledged by NCA and in the absence of any instruction to the contrary, a firm will be free to operate the customer's account under normal commercial considerations. This acknowledgement however does not indicate that the suspicion has been investigated or that it is unfounded.

If the enquiries uncover a crime the investigation will serve a Court Order on the firm to provide the records needed as evidence. NCA will make their own discreet enquiries and their investigation will be confidential. A firm cannot be sued for breach of confidentiality for making a report to NCA.

Where NCA give consent following a disclosure, this provides the staff involved with a defence against a charge of money laundering. It is not intended to over-ride normal commercial judgement and a firm is not committed to continuing the relationship with the customer if such action would place the reporting firm at commercial risk. However before terminating a relationship the firm should liaise with NCA or the investigating officer to ensure they do not inadvertently "tip off" the customer or prejudice the investigation.

Penalties

A person guilty of the offence of failure to disclose is liable to a fine or to imprisonment or both. They could also be found guilty of money laundering itself which has a maximum imprisonment of 14 years.

Tipping off

It is an offence for any person if they know or suspect a disclosure has been made to take any action likely to prejudice the investigation such as "tipping off".

Recognising suspicious transactions

Firms need to be able to recognise and report suspicious transactions. A person who considers a transaction to be suspicious would not be expected to know the exact nature of the criminal offence or that funds are definitely arising from the crime.

A firm's knowledge of their customers should help them to decide whether, taking into account what they know about them and their background whether the transaction is something unexpected or unusual. This in itself does not necessarily mean it is suspicious if there is a legitimate explanation.

Examples of factors which may give rise to suspicion:

<u>New business</u>

- A new corporate/trust client where there are difficulties and delays encountered in obtaining copies of accounts or other documents of incorporation where required.
- A personal lines customer for whom verification of identity proves unusually difficult or who is reluctant to give full details.
- A client using numerous offshore accounts, companies/structures in circumstances where the clients needs do not support such economic requirements.
- Any transaction using an undisclosed third party.
- A client who does seem interested in the performance or terms of the contract but is more interested in early cancellation of the contract.
- Transactions that have no apparent purpose and make no obvious economic sense.
- A request to insure goods in transit to or situated in countries where terrorism, the production of drugs, drug trafficking or organised crime may be prevalent.

<u>Payment</u>

- Payment of very large premiums with cash.
- Client purchases a policy which is considered beyond his apparent means.
- Over payment of a premium with a request to pay the excess to a third party.
- Payment in cash when the business transaction would typically be made by cheque, direct debit mandate (DDM) or credit card.
- A client who has always paid by cheque, credit card or DDM suddenly offering payment by cash.

- Unemployed or low paid customers arranging insurances with substantial premiums.

Abnormal transactions

- Assignment of a policy to an unrelated third party.
- Early cancellation of policies in circumstances which generate a large return premium, particularly where they appear unusual or occur for no apparent reason.
- Cancellation and request for the refund to be paid to a third party especially where cash was tendered.
- Customers who regularly insure against a common risk and make a number of small claims.
- Cancellation of a number of policies taken out by an insured, especially where the premium refund is made to a third party.
- Customers who make a practice of early cancellation.
- Claims paid to persons other than the insured.
- Change of ownership on a policy just before a loss occurring.

In addition to the above, firms should also be able to recognise and report any matters concerning employee fraud.

2.10.4 Data Security

Customer data is a high value commodity for fraudsters and firms have a responsibility for securing it.

What is customer data?

Customer data is any personal information held in any format. It includes National Insurance records, addresses, dates of birth, family circumstances, bank details and medical records. This information must be kept secure because fraudsters can use it to commit crimes such as identify theft.

There is a misconception that the compromise of customer data is purely an IT issue. Customer data can in fact, be compromised in a number of ways.

Ensuring physical security over customer data

Physical security should be appropriate to prevent unauthorised access to customer data.

Many firms are responsible for their own office security. Firms should assess the risk of unauthorised access to their premises and to ensure there is a commensurate level of security to protect your customer data.

Firms may wish to consider:

- Installing alarms or CCTV;
- Restricting access to the office with use of door buzzers or keypad entry;
- Monitoring visitors to your office by recording access and departure with a signing in book and supervising visitors to your premises at all times;
- Discussing with local businesses or your local police force the key security risks in your area;
- Raising staff awareness of the risks of poor physical security;
- Maintaining a clear desk or secure desk policy to reduce the risk of customer data being lost, stolen or accessible to unauthorised persons; and
- Keeping filing cabinets locked whilst not in use.

Governance

Senior management should assess data security and put in place appropriate policies, procedures and controls to reduce the risks relating to it.

Data security is often not considered as a specific risk and can mean that nobody is assigned responsibility for it. In addition many firms treat data security as purely an IT issue and therefore do not involve other key staff from across the business such as those responsible for recruitment, security and countering financial crime.

The FCA do not expect small firms to spend as much money or resource on data security as larger firms. However they do expect firms to assess the risks and to have written data security policies or procedures. These do need to be appropriate to the size of the business and the risk posed and often a simple set of “do’s” and “don’ts” would suffice.

You should also consider whether the culture within the firm is such that staff would be encouraged to report data security issues or concerns and whether staff understands why it is important and the steps they need to take to keep customer data safe.

Staff Recruitment

Firms recruitment processes should ensure that the staff you recruit are not susceptible to stealing data or committing fraud.

In most firms it is the staff in the more junior roles such as “contact centre” staff or administrators who tend to have access to most customer data and therefore present a higher risk in terms of potential data loss or theft. There are also a number of cases where junior staff have been bribed or threatened by criminals who wish to obtain customer data. Firms should be applying a risk-based approach to reducing financial crime and enhancing recruitment checks where appropriate. Firms should consider whether it would be appropriate to:

- Undertake credit or criminal record checks on staff with access to large amounts of customer data;
- Repeating credit checks periodically to ensure that staff in financial difficulties who may be more susceptible to bribery or committing fraud and managed appropriately; and
- Hold regular meetings with staff where firms can identify any changes in circumstances which might make an employee more susceptible to financial crime.

Training

Firms need to ensure that staff understands the importance and relevance of data security policies and procedures. It is not sufficient for firms to place reliance on staff stating that they have read policies and procedures, they should be confirming that they understand.

There are many simple and effective means of raising staff awareness such as: group discussions, awareness raising emails, intranet sites and poster campaigns. In addition firms should ensure that they regularly test staff’s understanding of data security.

Systems and Controls

There are many systems and controls which can minimise risks to customer data. Examples follow:

Access rights to IT systems

Firms should consider:

- Whether staff have access rights to customer data that they do not require;
- Are unnecessary access rights removed if staff change roles; and
- Risk based proactive monitoring of staff to ensure that they are accessing or amending data for genuine business reasons.

Passwords and User accounts

Firms should consider:

- Whether all staff have their own username and password;
- Whether passwords meet the standards recommended by Get Safe Online (www.getsafeonline.org)
- Whether staff understand the importance of strong passwords; and
- Whether passwords are written down or shared.

Taking Customer Data Offsite

If firms have staff who work from home or use laptops and other portable devices such as memory sticks and CDs to store or transfer data then they should be considering the risks to customer data that could arise from these situations and in particular the loss or theft of a laptop or portable device.

Firms should consider:

- Where customer data taken offsite, is it or the device encrypted?;
- Maintaining records of who has laptops, memory sticks or CDs to ensure that should one go missing firms would be aware;
- Random checks of laptops to ensure that only staff authorised to hold customer data on laptops are doing so;
- If staff use home computers for business purposes how securely is customer data held; and
- Ensure they are aware of the increasingly sophisticated and evolving mobile technology.

Backing up customer data

Firms should consider reviewing their back procedures and consider threats to customer data throughout the whole back up process from production of the tape or disk through the transit process to the ultimate place of storage.

Firms should consider:

- Whether there are agreed and consistent procedures for back up of customer data;
- Whether the storage facilities are sufficiently secure to minimise risks to customer data;
- Encrypting backed up data;
- Carrying out due diligence on any third party entrusted with storage of back up data; and
- If a member of staff holds backed up data overnight how secure is the storage.

Internet and Email Availability

There is an increased risk to data security if internet and external email are used in an uncontrolled fashion and especially where staff have access to web-based communication facilities such as: web-based email (hotmail), social networking sites, instant messaging and file sharing software.

There firms should consider:

- Providing access to the internet and external email only where it is genuinely required; and
- Removing access to web-based communication facilities and file sharing software.

Disposal of Data

Customer data can be held in paper and electronic forms and firms should ensure that all customer data is disposed of in a secure manner.

Firms should consider:

- Shredding paper based customer data and reminding staff of the importance of this;
- Ensuring that if you use a third party to dispose of customer data that you are aware of how they destroy data and that they have rigorous vetting process when recruiting staff;
- Computer disks and CDs should be destroyed or shredded prior to disposal; and
- When disposing of computers ensuring that hard drives are destroyed of specialist software is employed to wipe the data.

Third Party suppliers

Many firms employ third-party suppliers to carry out IT support or office cleaning and security. This can lead to people outside the firm having access to customer data.

Firms should:

- Undertake good due diligence on third party suppliers to assess their policies and procedures, including recruitment, security and levels of service to ensure that firms understand their obligations with respect to how they treat your customer data;
- Monitor and supervise access to offices and customer data
- Operate a clear desk or secure desk policy; and
- Lock filing cabinets when not in use; and
- Use secure internet links, encryption and registered/recorded mail when transferring data.

Compliance and Monitoring

Firms should ensure that data security policies and procedures are reviewed on a regular basis.

2.11 Anti-Bribery and Corruption

The Bribery Act 2010 came into force on 1 July 2011. It applies to all commercial organisations, whether in the public or private sector, regardless of size, with operations in the UK. This includes overseas companies with a presence in the UK. It affects all insurance intermediaries.

The Act creates four new criminal offences:

- giving, promising or offering a bribe (section 1)
- requesting, agreeing to receive or accepting a bribe (section 2)
- bribing a foreign public official (section 6)
- failure by a commercial organisation to prevent active bribery being committed on its behalf

As a minimum, firms need to have "adequate procedures" (see below) to prevent bribery being committed on their behalf.

2.11.1 What is a bribe?

The Act defines a "bribe" widely, as a "financial or other advantage". It includes obvious things like cash payments, but could also include gifts, corporate hospitality, letting someone off an existing debt or providing someone with free services.

The key point about a bribe is that it must be "improper", where the "financial or other advantage":

- is intended to make someone perform a function or activity improperly, or reward them for having done so; or
- is offered or given knowing that it would be improper for them to accept it.

Some factors to take into account when deciding whether a payment or advantage is improper are:

Factors suggesting no impropriety	Factors suggesting impropriety
Payment / benefit is proportionate, having regard to an existing or potential business relationship	Payment / benefit seems excessive, having regard to an existing or potential business relationship
Payment / benefit is given openly and transparently	Payment / benefit is concealed
Payment is fair compensation for services provided	Payment is disproportionate to services provided
Payment / benefit is consistent with accepted market practice	Payment / benefit goes beyond accepted market practice
Benefit complies with internal policies of both giver and receiver	Benefit breaches internal policies of either giver or receiver
Payment is required by law or agreed in a written contract	Payment is described as a fee or otherwise suggesting it is legally required when it is not
Benefit is freely offered by the giver (without improper intent)	Payment / benefit is demanded but is not legally or contractually required
Benefit is given to a recipient already well-known to the payer	Payment / benefit goes to a recipient with whom the payer has no pre-existing relationship
Benefits are given equally to a pool of individuals	Benefits are targeted exclusively at key decision makers

Where one or more of the factors suggesting impropriety are present, firms may wish to consider whether the decision to proceed be taken at a more senior level by someone independent.

Gifts and corporate hospitality

The Government's guidance makes it clear that it "does not intend for the Act to prohibit reasonable and proportionate hospitality and promotional or other similar business expenditure".

Gifts and hospitality should be proportionate to the seniority and status of the recipient. Firms should have regard to both their own corporate policy on gifts and that of the proposed recipient. In the case of some public bodies the threshold may be very low. Indeed, some public or government bodies may

prohibit their staff entirely from receiving gifts or hospitality. There should be a justifiable business reason for giving the gift or hospitality to that recipient.

An important consideration will be the accepted 'norm' for the market in which the firm operates. Firms also need to consider possible reputational risk and their obligation to manage conflicts of interest fairly. Firms should set levels for gifts or hospitality above which there is a need for additional senior management approval, prior to sign off.

Case studies:

A has enjoyed a particularly successful year, and decides to reward the companies that are its key introducers of business with a case of non-vintage champagne each.

Assuming that the champagne is likely to be shared among a number of individuals at each recipient company, the total value to each individual is likely to be relatively small. It is therefore less likely to induce those receiving it to act improperly in favour of A in the future. For added reassurance, A could check the gifts policy of the recipient companies.

B decides it wants to target a large potential new client. Having identified the head of procurement as the key person to target, it offers her and her family an all-expenses trip to the Champagne region of France.

There are several factors here which might suggest impropriety, such as the targeting of a single individual, the fact that there appears to be little or no existing business relationship, and the size of the gift including extending it to her family, which would appear to be disproportionate. This could therefore be a bribe given in order to secure a new client. B should consider whether the scale of the benefit is appropriate, having regard to what B and its competitors would regard as normal market practice, and record the decision that it makes.

Commissions

Commissions which are payments in return for services provided are unlikely to be bribes, as there is nothing improper about them. However, a payment received by a broker in breach of its duties to its customer under the law of agency is likely to be regarded as "improper" for the purposes of the Act. A payment significantly in excess of the value of any service provided could also be a bribe or some other improper payment disguised as commission.

Firms should consider whether the level of a commission reflects the value of the service to be provided in return. Even if it is the "market rate", it could still be regarded as a bribe if it is intended to induce the person receiving the commission to act improperly – for example, in breach of their duty to their client.

Firms should have a documented policy on how commission rates are arrived at and approved, and records that show this policy being applied in practice.,

The link between bribes and inducements

There is an overlap with the requirement under ICOBS 2.3 on firms to avoid conflicts of interest, in particular in relation to inducements.

However, while ICOBS 2.3 is concerned with the propriety of an inducement as between a broker and its customers, the Bribery Act would look at an inducement from the perspective of the broker and the insurer or other third party which is giving or receiving the inducement. So while in many cases a bribe will also be a breach of ICOBS 2.3, the range of possible offences under the Bribery Act is wider in scope than conflicts of interest under ICOBS. Equally, an arrangement may be entirely "proper" for the purposes of the Bribery Act, but still give rise to a conflict of interest under ICOBS.

This means that firms should consider commissions and other arrangements between brokers and insurers and other third parties in the light of both ICOBS 2.3 *and* the Bribery Act. Compliance with one does not automatically mean compliance with the other.

Payments to third parties

Firms should also be wary of payments made to others, including payments made at the request of those that you do business with. It may be that, unknown to you, the person asking you to make that payment is related to the third party, or benefiting from the payment in some other way. These might include charitable or political donations or sponsorship agreements. If asked to make such payments, firms should carry out checks on the third party to ensure that they are legitimate.

Ownership of bank accounts

Firms should take care to check that where someone provides them with details of a bank account into which to make payments, the account is in fact owned and controlled by the person or company for which the payment is intended. This might include verifying the details with another person at the organisation, such as the Finance Director, or requiring the other party to provide an original bank statement from the third party showing the sort code, account number and name of account holder. A copy of any evidence obtained should be kept on file.

Is there an exemption for facilitation payments?

There is no exemption under the Act for so-called "facilitation payments" (small level payments made to officials to ensure that they perform a particular function, or perform it more quickly).

The UK Government recognises in its guidance that eradication of facilitation payments is "a long term goal" in some parts of the world and in certain sectors. The Serious Fraud Office (**SFO**), the main prosecuting authority for offences under the Bribery Act, has said that it will exercise its discretion in deciding whether to prosecute in such cases. In particular, where an organisation self-reports, and where it has a clear and appropriate policy which has been followed, these are factors which would point the SFO away from prosecution. However, large or repeated payments, and/or a failure to follow an organisation's own policies would be more likely to lead to a prosecution.

Payments for legally required administrative fees or fast-track services are not facilitation payments.

2.11.2 When does the Act apply?

The Act applies to bribes offered, promised or given not just to government officials, but to employees of other businesses a firm may deal with, or others who are in a position of trust. These might be commercial insureds, insurers, or others who you deal with in the course of your business. The Act also makes it an offence to ask for, agree to receive or accept a bribe. It applies wherever in the world a firm does business, or where others do business on its behalf.

Actions of employees' and others providing a service?

A business is responsible for their employees' actions and could be found guilty of the criminal offence of failing to prevent bribery if its employees (or others), offer or pay bribes in the course of their employment. This is a "strict liability" offence, which means a business could be found guilty even if it did not know the bribe was being offered or paid. The only defence is to show that the firm has "adequate procedures" to prevent bribery.

Firms are also responsible for making sure that anyone who provides a service for them or on their behalf (an "associate") does not offer or pay a bribe with the intention of winning business for them, or getting an advantage for their business. This will include third parties who help win business for them, joint venture partners and outsourcing partners who perform a service on their behalf. This means that firms will need to check what they are doing to comply with the Act. A business could be liable for failing to prevent them from offering or paying bribes, even if they did so without its knowledge or approval.

If business comes to a firm through a chain of intermediaries, it cannot claim to be only responsible for the last in the chain before them. Similarly, if the firm outsource a particular operation, it may also be responsible for the services performed for by sub-contractors of the party that it has contracted with.

2.11.3 What are "adequate procedures"?

The only defence to a charge under section 7 of the Act is to be able to show that the firm has "adequate procedures" in place to prevent bribery being committed on behalf of its business. The Ministry of Justice has prepared guidance on what might amount to adequate procedures. This guidance does not provide a "safe harbour", so following it will not guarantee immunity from prosecution. But if a firm can show that it acted in accordance with the guidance, it is likely to help its case significantly.

Like FCA requirements, a firms' procedures should be proportionate to the risk posed and should take into account the size and complexity of business undertaken.

2.11.4 Consequences of getting it wrong?

Individuals could be sent to jail for up to ten years, and individuals and businesses could be hit with an unlimited fine. Senior officers within a company who have consented to or connived in bribery would face the same punishments.

In addition there is the potential for reputational damage and an investigation into alleged bribery or corruption could also take up a lot of management time, even if it does not result in prosecution. A firm would also need to report any investigation to the FCA which may result in the FCA questioning whether the firm and/or its approved persons can continue to be regarded as fit and proper. A bribery conviction could also rule out a firm from tendering to an EU government or local authority in the awarding of public contracts.

Who prosecutes bribery offences?

Currently there are several agencies within the UK which investigate and enforce offences of bribery and corruption. The SFO is the lead authority in the UK for domestic and overseas bribery and corruption.

The City of London Police has a dedicated Fraud Desk, which one can call to seek advice or report any suspicion of a crime within the City of London. They will also investigate potential offences under the Bribery Act 2010. The City of London Police also has a dedicated Overseas Anti-Corruption Unit which often works closely with the SFO in investigating and prosecuting offences.

The National Crime Agency may become involved in investigations where there is a serious or organised criminal element. Similarly, Revenue and Customs Prosecutions Office (now part of the Crown Prosecution Service) could also have a role to play in relevant cases.

The Act provides that a prosecution cannot be started unless it is by or with the consent of a limited number of senior prosecutors. That should help to ensure that sensible judgments are exercised about whether to prosecute possible offences under the Act.

What should you do if you come across possible bribery?

If you come across a possible case of bribery, do not ignore it. If an employee, agent or anyone else providing services for you or on your behalf breaches your anti-bribery and corruption policy, it may be appropriate to take disciplinary proceedings against them. In the case of a third party, it may call into question whether you still want to do business with them.

But it may be that the incident shows that your training was not sufficient, or that your internal controls were inadequate. Make sure that you learn the lessons to prevent a recurrence. For example, the case may show that you have underestimated the risk from a particular area of business.

It is important that you have an effective internal whistle-blowing system, so that staff know who to report any concerns to internally and can do so in confidence. This also ensures that any issues are dealt with by a senior member of staff.

Should we report to the authorities?

The question of whether to report an incident or suspicion to the FCA or one of the prosecuting authorities can be a complicated one, as it often depends on the circumstances. A firm may need to obtain legal advice on how best to proceed. The SFO has said it will look favourably on companies that self report cases of bribery to it. The SFO has published guidance on its website on this issue at http://www.sfo.gov.uk/bribery--corruption/corporate-self-reporting.aspx

Who should we report to?

Generally, any report of suspected bribery or corruption would be made to the SFO. The SFO's anticorruption team will decide if the matter is best dealt with by the SFO or whether to pass it on to one of the other agencies, such as City of London Police. Alternatively, if you think you may have been a victim of financial crime, you might want to report it to the City of London Police or to NCA. In either case, you should consider whether you should also report the matter to the FCA, depending on the circumstances.

Reports to the SFO can be made via its website at:
https://report.sfo.gov.uk/sfo-confidential---provide-information-in-confidence.aspx
or in writing to:
SFO Confidential, Serious Fraud Office, 2-4 Cockspur Street, London, SW1Y 5BS. The SFO does not take reports over the telephone.

The City of London Police can be contacted at:
Action Fraud: 0300 123 2040

Anti-Corruption Unit
Overseas Anti-Corruption Unit Reporting Line 020 7601 6969
(This is a 24/7 confidential answer phone service which allows the caller to report their suspicions either openly or anonymously)

Email: OACU@cityoflondon.police.uk

Address:
Overseas Anti-Corruption Unit (OACU)
City of London Police
4th Floor, 21 New Street
London EC2M 4TP

What is the FCA's involvement in the Bribery Act?

Bribery and corruption is classed by the FCA as financial crime. In May 2010, the FSAs, as it was known, published a report highlighting good and bad practice in this area. This report can be found on the FCA website:
http://www.fca.org.uk/static/documents/fsa-anti-bribery-report.pdf.

They found the following weaknesses:

- weak governance of anti-bribery and corruption and a poor understanding of bribery and corruption risk among senior managers;
- poor responses by many firms to significant bribery and corruption events which should have led them to reassess the adequacy of their preventative systems and controls;
- weak monitoring of third party relationships and payments with a worrying lack of documentary evidence of due diligence taking place;
- little or no specific training provided on anti-bribery and corruption, even for staff in higher risk positions; and
- inadequate compliance and internal audit monitoring of anti-bribery and corruption work.

Firms should review the following areas:

- Proportionate procedures to prevent bribery
- Governance and management information;
- Risk assessment and responses to significant events;
- Due diligence on third party relationships;
- Payment controls;
- Staff recruitment and vetting;
- Training and awareness;
- Remuneration structures and associated risks;
- Incident reporting; and
- Role of compliance and internal audit.

Proportionate Procedures

A firm should have proportionate procedures in place to prevent bribery by persons associated with it. These should be based on the bribery risks it faces and the nature, scale and complexity of its activities. They must be clear, practical, accessible, effectively implemented and enforced.

Firms should:

- Review and amend guidance on hospitality, corporate gifts, sponsorship, charitable and political donations and other payments to third parties.
- Check existing payment authorisation processes and mechanisms for flagging unusual payments.
- Clearly communicate to staff and those who perform services on your behalf your ethical business values.
- Your policy and procedures should be easy to access and understand, and relevant to your business.
- Put in place procedures to manage incidents of bribery.

Governance and Management Information

Senior management awareness, involvement and responsibility are vital in ensuring adequate anti-bribery and corruption systems and controls are in place and that appropriate resources are allocated to mitigate identified risks. Senior management need to demonstrate their commitment to preventing bribery and foster a culture where bribery in never acceptable.

Firms should have:

- Clear and documented responsibility for anti-bribery and corruption apportioned to a senior manager or committee. If it is apportioned to a committee then this should have senior management membership, appropriate terms of reference and should report to the Board.
- Good Board level and senior management understanding of the bribery and corruption risks faced by the firm including the materiality to the firm and how to apply a risk based approach.
- Swift and effective senior management led responses to significant bribery and corruption events, which highlight potential areas of improvement in systems and controls.
- Regular MI to the Board and senior management, covering new third party accounts and their risk classification, higher risk third party payments for the preceding period, changes to third party bank account details, unusually high commission paid to third parties and general information about external developments relating to bribery and corruption.
- Actions taken or proposed in response to issues highlighted by management information to be documented and acted on.
- Consider a public statement of commitment to counter bribery.
- Ensure internal communications come from board level.

Risk Assessment and Responses to Significant Events

Firms should:

- Identify the parts of their business which are most exposed to bribery.
- Identify the types of transactions which are most vulnerable.
- Undertake regular assessments of bribery and corruption risks taking into account the country and class of businesses involved as well as other relevant factors.
- Perform more robust due diligence tests and monitoring of higher risk third party relationships.
- Conduct thorough reviews and gap analyses of systems and controls against relevant external events with strong senior management involvement or sponsorship.
- Ensure review teams have sufficient knowledge of relevant issues and where necessary supplementing their knowledge with external expertise.
- Have clear plans in place to implement improvements resulting from reviews.
- Have adequate and prompt reporting to NCA and to the FCA of any inappropriate payments identified during reviews.
- Look at payments to third parties – why are they made, how are they approved, and how do you satisfy yourself that they are commensurate with services provided?
- Review how clients and potential clients are entertained and rewarded.
- Identify joint ventures, intermediaries, outsources and other sources of business, who might put you at risk.
- Consider whether your pay structures, such as bonuses, encourage staff to commit bribery or corruption.
- Identify any jurisdictions you may deal with where the bribery and corruption risks are higher.

Due Diligence of Third Party Relationships

This was an area of considerable concern for the FCA and in particular:

- Over reliance on informal market view of integrity of third parties.
- No detailed checking of high risk third parties to ensure that they were not connected to assured, clients or public officials.
- No documented business case for using third parties.
- No regular reviews of third parties.
- No review of third parties as part of acquisitions.
- No consideration as to whether third party payments were commiserate with services provided.
- Making payments to others on instructions of third parties.
- No independent checking of third party due diligence.
- No central list of third parties.
- Inadequate steps taken to confirm the third parties bank account.

Firms should:

- Maintain a central list of third parties used to obtain or retain business.
- Have documented policies with a clear definition of what constitutes a 'third party' and the due diligence required when establishing and reviewing any arrangement.
- Perform more robust due diligence checks of higher risk third parties including a detailed understanding of the business case for using them.
- Have a clear understanding of the roles clients, directors, reinsurers, solicitors and loss adjustors play in transactions to ensure they are not carrying out higher risk activities.
- Use third party forms that ask relevant questions, clearly stating these are mandatory.
- Review third party account open forms and ensuring they are approved by a relevant person or committee such as compliance or risk.
- Use commercially available intelligence tools and databases and/or other research techniques to check third party declarations about connections to public officials, clients or the assured.
- Inform all parties involved in the insurance transaction about the involvement of third parties being paid commission.
- Ensure current third party due diligence is appropriate when business is acquired which is higher risk that existing business.
- Set commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business. In addition considering paying a one off fee to third parties where the role is purely introducing.

- Ensure all relevant employees understand the definition and the due diligence required in relation to establishing and maintaining relationships with third parties, particularly if they are higher risk. Firms should initially regard all companies and/or individuals involved in insurance transactions who are not the underwriter or the assured to be third parties.
- Consider which types of third parties pose the greatest risk of bribery and corruption, and take this into account when refining the definition.
- Take reasonable steps to ensure that bank accounts used by third parties are in fact controlled by the third party for which the payment is meant. For example brokers may wish to see third party bank account statements or ask the third party to write them a low value cheque.
- Undertake higher or extra level checks for higher risk third parties.
- Regularly reviewing third party relationships to identify the nature and risk profile.
- Maintain a central record of approved third parties, the due diligence undertaken and evidence of periodic reviews.

Third parties who provide services to refer, assist or facilitate the introduction of the client or the assured are likely to pose a higher risk of bribery and corruption. There is likely to be an increased risk of a third party being the recipient of a bribe or paying a bribe to others from commission received if:

- It is an individual (or a 'company' which is in fact an individual) – this is because an individual is more likely to be the ultimate recipient of a bribe and, generally, it is likely to be more difficult for an individual to influence a client to place insurance business with a particular broker firm.
- It is introducing business from a country which is higher risk from a bribery and corruption perspective – paying bribes can be regarded as 'how business is done' in some higher risk countries and there could be inadequate anti-bribery and corruption legislation and/or enforcement of it.
- It is connected to the assured, the client or a public official – this increases the risk that corrupt means could be used to win business, particularly if those to whom the third party is connected have influence over procurement decisions.
- There is no convincing business case for the third party to receive commission or the amount of commission paid appears high compared with the amount of work they do. It is important for firms to understand fully the role of a third party and the services they provide so they can satisfy themselves that they are not making or becoming involved in illicit payments where the case for paying a third party is unclear.
- It is paid commission on the instructions of another party involved in the transaction. In these circumstances, broker firms could be being used by another individual or entity to pay bribes to the third party.

- The third party does not want others involved in the transaction to know it will receive commission. This lack of transparency increases the likelihood of bribery and corruption.
- The third party requires payment of commission in advance of premiums being paid. Here, there is a risk that the commission could either be a bribe or passed on to others as a bribe to secure the business.

Examples of third parties likely to pose a lower risk of bribery and corruption are brokers, clients, reinsurers, solicitors and loss adjusters who are regulated within the EEA or by the FCA. However, there are situations where these types of third parties carry out higher risk activities such as introductions or referrals. It is therefore essential that firms clearly understand the role of third parties such as clients, reinsurers, solicitors and loss adjusters in all transactions, and define and treat them as a higher risk third party where appropriate.

Payment Controls

Firms should:

- Ensure adequate due diligence and approval of the third party relationship before any payments are made.
- Have a risk-based approval process for payments and a clear understanding of why they are being made.
- Check payments individually prior to approval to ensure consistency with the business case for the account.
- Undertake regular and thorough monitoring of third party payments to check for example whether the payment is unusual.
- Have a healthily sceptical approach to approving third party payments.
- Have adequate due diligence on new suppliers.
- Set clear limits on staff expenditure, which are fully documented, communicated and enforced.
- Limit third party payments to reimbursement of genuine business costs or reasonable entertainment.
- Ensure reasons for third party payments are clearly documented and appropriately approved.
- Be able to easily produce a list of all payments made to third parties.
- Produce accurate management information to facilitate effective payment monitoring.

Staff Recruitment and Vetting

Firms should:

- Vet staff on a risk-based approach taking into account the financial crime risk.
- Have in place enhanced vetting for staff with higher bribery and corruption risks. This could include:
    - credit checks;
    - criminal record check; and/or
    - financial sanction check and commercially available intelligence databases including CIFAS Staff Fraud Database.
- Have a risk based approach for dealing with adverse information raised by vetting checks.
- If using employment agencies to recruit staff in higher risk positions have a clear understanding of the checks they carry out and periodically check that the agencies are in fact complying with the agreed vetting standards.
- Implement a formal process for identifying changes in existing employees' financial soundness.

Training and Awareness

Firms should:

- Provide good quality standard training on anti-bribery and corruption to all staff and additional training to those staff in higher risk positions.
- Consider extending training to joint venture partners, distributors and other associates.
- Ensure those undertaking the training have had adequate training themselves.
- Ensure training covers practical examples of risk and how to comply with policies and procedures.
- Test staffs' understanding and use the results to assess individual training needs and the overall quality of the training.
- Maintain complete staff training records.
- Ensure penalties for non-compliance are clear.
- Check whistleblowing procedures are in place.
- Ensure internal compliance documentation is up to date and incorporated into contracts of employment.
- Provide refresher training and ensure that it is kept up to date.

Incident Reporting

Firms should:

- Have in place clear whistleblowing and reporting of suspicions procedures and ensure these are communicated to staff including:
    - Appointment of a manager to oversee the process and be the main point of contact for staff with concerns regarding their line manager.
    - Respect the confidentiality of those who raise concerns.
- Have internal and external suspicious activity reporting procedures.
- Keep records of internal suspicious activity reports
- Ensure training covers suspicious activities and how to report them.

Role of Compliance and Internal Audit

Firms should:

- Ensure compliance and internal audit staff receive specialist training.
- Have effective compliance monitoring and internal audit reviews which challenge not only whether the processes mitigate bribery and corruption have been followed but also whether the processes themselves are effective.
- Where appropriate have independent checking of compliance's role in approving third party relationships and accounts.
- Routinely undertake compliance and/or internal audit checks of higher risk third party payments to ensure there is appropriate supporting documentation and adequate justification.
- Review your policy regularly: at least once a year, or when there is a significant change in your business.
- Put in place an auditing system to check that staff and associates follow your procedures.
- Make sure adequate records are kept – they are your first line of defence.
- Carry out a bribery and corruption risk assessment when considering moves into new products or territories, or business acquisitions.
- Consider getting external validation of your procedures.
- Be sure to learn the lessons from any incidents that do occur – identify the root cause and ways to prevent a recurrence.
- Review the MI that is provided on anti bribery and corruption to ensure that it remains fit for purpose.
- Monitor publications on this topic from the regulator and updates from trade bodies.

Record keeping

It is important that a firm keeps records that show that they are complying with policy and procedures. For example, if corporate hospitality above a certain level requires sign-off at a senior level, there should be records that demonstrate that the firm has complied with that policy in practice. Similarly, board minutes should record that anti-bribery and corruption issues have been considered at a board level, and training records should show who has attended anti-bribery and corruption training. Records should also identify every time the policy and procedures have been reviewed, whether in response to a particular event or incident, or just on a rolling basis to ensure that it remains up-to date.

2.12 Financial Sanctions

What are financial sanctions?

Financial sanction orders prohibit a firm from carrying out transactions with a person or organisations (known as the target). This applies to all transactions; there is no minimum limit.

The HM Treasury (HMT) maintains a list of targets, known as the UK Consolidated Financial Sanctions List (HMT list). A breach of a financial sanctions order may be a criminal offence.

There are about 50 UK individuals and 12 UK entities on the current HMT list and most of these individuals or entities know they are on the list so the issue of "tipping off" should not generally arise.

What should firms do?

Firms should check:

- Existing clients against the HMT's list, this can be found at www.hm-treasury.gov.uk/financialsanctions ;
- All new customers prior to providing any services or transactions;
- Updates to the list on a regular basis; and
- Any changes to your client's details.

It is also good practice to include directors, beneficial owners of corporate customers and any third party payees in your checks.

What do should firms do if one of their clients is on the HMT list?

If a firm finds that one of their clients is on the list then they are required to stop any services provided to the client and report the matter as soon as possible to:

HMT's Asset Freezing Unit at:
Asset Freezing Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ