Chapter 2

Financial crime systems and controls

2

2.1 Introduction

2.1.1 G **Who should read this chapter?** This chapter applies to **all firms** subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R. It also applies to e-money institutions and payment institutions within our supervisory scope.

2.1.2 G The Annex I *financial institutions* which we supervise for compliance with their obligations under the *Money Laundering Regulations* are not subject to the financial crime rules in *SYSC*. But the guidance in this chapter applies to them as it can assist them to comply with their obligations under the Regulations.

2.1.3 G All firms must take steps to defend themselves against financial crime, but a variety of approaches is possible. This chapter provides guidance on themes that should form the basis of managing financial crime risk. The general topics outlined here are also relevant in the context of the specific financial crime risks detailed in subsequent chapters. See SYSC 6.1.1R and SYSC 3.2.6R.

2.2 Themes

Governance

2.2.1 G We expect **senior management** to take **clear responsibility** for managing financial crime risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are **actively engaged** in the firm's approach to addressing the risks. In considering senior management arrangements in the Guide, firms should consider their arrangements to comply with the Senior Managers and Certification Regime (SM&CR).

[**Editor's note:** see https://www.fca.org.uk/firms/senior-managers-certification-regime]

Self-assessment questions:

- When did senior management, including the board or appropriate sub-committees, last consider financial crime issues? What action followed discussions?
- How are senior management kept **up to date** on financial crime issues? (This may include receiving reports on the firm's performance in this area as well as ad hoc briefings on individual cases or emerging threats.)
- Is there evidence that **issues have been escalated** where warranted?

Examples of good practice	Examples of poor practice
• Senior management **set the right tone** and demonstrate leadership on financial crime issues.	• There is little evidence of senior staff **involvement** and **challenge** in practice.
• A firm takes **active steps** to prevent criminals taking advantage of its services.	• A firm concentrates on **narrow compliance** with **minimum regulatory standards** and has little engagement with the issues.
• We would draw comfort from seeing evidence that these practices take place.	• Financial crime issues are dealt with on a purely **reactive** basis.
• A firm has a strategy for self-improvement on financial crime.	• There is **no meaningful record** or evidence of senior management considering financial crime risks.
• There are clear criteria for **escalating** financial crime issues.	

2

Management information (MI)

2.2.2 G MI should provide senior management with **sufficient information** to understand the financial crime risks to which their firm is exposed. This will help senior management effectively manage those risks and adhere to the firm's own risk appetite. MI should be provided regularly and ad hoc, as risk dictates.

Examples of financial crime MI include:

- an overview of the financial crime risks to which the firm is exposed, including information about emerging risks and any changes to the firm's risk assessment
- legal and regulatory developments and the impact these have on the firm's approach
- an overview of the effectiveness of the firm's financial crime systems and controls
- an overview of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected, and
- relevant information about individual business relationships, for example:
  - the number and nature of new business relationships, in particular those that are high risk
  - the number and nature of business relationships that were terminated due to financial crime concerns
  - the number of transaction monitoring alerts
  - details of any true sanction hits, and
  - information about suspicious activity reports considered or submitted, where this is relevant.

MI may come from more than one source, for example the compliance department, internal audit, the MLRO or the nominated officer.

Structure

2.2.3 G Firms' **organisational structures** to combat financial crime may differ. Some large firms will have a single unit that coordinates efforts and which may report to the head of risk, the head of compliance or directly to the CEO. Other firms may spread responsibilities more widely. There is no one 'right answer' but the firm's structure should promote coordination and information sharing across the business.

Self-assessment questions:

- Who has ultimate **responsibility** for financial crime matters, particularly: a) anti-money laundering; b) fraud prevention; c) data security; d) countering terrorist financing; e) anti-bribery and corruption and f) financial sanctions?
- Do staff have **appropriate seniority** and **experience**, along with clear reporting lines?

- Does the structure promote a **coordinated approach** and **accountability**?

- Are the firm's financial crime teams **adequately resourced** to carry out their functions effectively? What are the annual budgets for dealing with financial crime, and are they **proportionate** to the risks?

- In smaller firms: do those with financial crime responsibilities have **other roles**? (It is reasonable for staff to have more than one role, but consider whether they are spread too thinly and whether this may give rise to conflicts of interest.)

Examples of good practice	Examples of poor practice
• Financial crime risks are addressed in a **coordinated** manner across the business and information is shared readily.	• The firm makes no effort to understand or address **gaps** in its financial crime defences.
• Management responsible for financial crime are **sufficiently senior** as well as being credible, independent, and experienced.	• Financial crime officers are relatively **junior** and lack access to senior management. They are often **overruled** without documented justification.
• A firm has considered how counter-fraud and anti-money laundering efforts can **complement** each other.	• Financial crime departments are **under-resourced** and senior management are reluctant to address this.
• A firm has a strategy for self-improvement on financial crime.	
• The firm bolsters insufficient in-house knowledge or resource with **external expertise**, for example in relation to assessing financial crime risk or monitoring compliance with standards.	

Risk assessment

2.2.4 G A **thorough understanding** of its **financial crime risks** is key if a firm is to apply proportionate and effective systems and controls.

A firm should identify and assess the financial crime risks to which it is exposed as a result of, for example, the products and services it offers, the jurisdictions it operates in, the types of customer it attracts, the complexity and volume of transactions, and the distribution channels it uses to service its customers. Firms can then target their financial crime resources on the areas of greatest risk.

A **business-wide risk assessment** – or risk assessments – should:

- be comprehensive and consider a wide range of factors – it is not normally enough to consider just one factor

- draw on a wide range of relevant information – it is not normally enough to consider just one source, and

- be proportionate to the nature, scale and complexity of the firm's activities.

Firms should build on their business-wide risk assessment or risk assessments to determine the level of risk associated with **individual relationships**. This should:

- enable the firm to take a holistic view of the risk associated with the relationship, considering all relevant risk factors, and

- enable the firm to apply the appropriate level of due diligence to manage the risks identified.

The assessment of risk associated with individual relationships can inform, but is not a substitute for, business-wide risk assessments.

Firms should regularly review both their business-wide and individual risk assessments to ensure they remain current.

Self-assessment questions:

- What are the main financial crime **risks** to the business?

- How does your firm seek to **understand** the financial crime risks it faces?

- When did the firm last **update** its **risk assessment**?

- How do you **identify new or emerging** financial crime risks?

- Is there evidence that risk is considered and recorded systematically, assessments are updated and **sign-off** is appropriate?

- Who **challenges** risk assessments and how? Is this process sufficiently rigorous and well-documented?

- How do **procedures** on the ground adapt to emerging risks? (For example, how quickly are policy manuals updated and procedures amended?)

Examples of good practice	Examples of poor practice
• The firm's risk assessment is **comprehensive**.	• Risk assessment is a **one-off** exercise.
• Risk assessment is a **continuous** process based on the best information available from internal and external sources.	• Efforts to understand risk are **piecemeal** and lack coordination.
• The firm assesses where risks are greater and **concentrates its resources** accordingly.	• Risk assessments are **incomplete**.
• The firm actively considers the **impact of crime** on customers.	• The firm targets financial crimes that affect the bottom line (e.g. fraud against the firm) but **neglects** those

Examples of good practice	Examples of poor practice
	where third parties suffer (e.g. fraud against customers).
• The firm considers financial crime risk when **designing new products** and **services**.	

Policies and procedures

2.2.5 G A firm must have in place up-to-date policies and procedures appropriate to its business. These should be **readily accessible**, **effective** and **understood** by all relevant staff.

Self-assessment questions:

- How often are your firm's policies and procedures **reviewed**, and at what level of **seniority**?
- How does it **mitigate** the financial crime risks it identifies?
- What steps does the firm take to ensure that relevant policies and procedures **reflect new risks** or **external events**? How quickly are any necessary changes made?
- What steps does the firm take to ensure that staff **understand** its policies and procedures?
- For larger groups, how does your firm ensure that policies and procedures are **disseminated** and **applied** throughout the business?

Examples of good practice	Examples of poor practice
• There is **clear documentation** of a firm's approach to complying with its legal and regulatory requirements in relation to financial crime.	• A firm has no **written policies** and **procedures**.
• Policies and procedures are **regularly reviewed** and **updated**.	• The firm **does not tailor** externally produced policies and procedures to suit its business.
• **Internal audit** or another independent party monitors the effectiveness of policies, procedures, systems and controls.	• The firm **fails to review** policies and procedures in light of events.
	• The firm **fails to check** whether policies and procedures are applied consistently and effectively.
	• A firm has not considered whether its policies and procedures are consistent with its obligations under legislation that forbids **discrimination**.

See SYSC 3.2.6R and SYSC 6.1.1R.

Staff recruitment, vetting, training, awareness and remuneration

2.2.6 G Firms must employ staff who possess the skills, knowledge and expertise to carry out their functions effectively. They should review employees' competence and take appropriate action to ensure they remain competent for their role. Vetting and training should be appropriate to employees' roles.

Firms should manage the risk of staff being rewarded for taking unacceptable financial crime risks. In this context, Remuneration Principle 12(h), as set out in SYSC 19A.3.51R and 19A.3.52E, may be relevant to firms subject to the Remuneration Code.

Self-assessment questions:

- What is your approach to **vetting** staff? Do vetting and management of different staff reflect the financial crime risks to which they are exposed?
- How does your firm ensure that its employees are aware of financial crime risks and of their **obligations** in relation to those risks?
- Do staff have access to training on an **appropriate range** of financial crime risks?
- How does the firm ensure that training is of **consistent quality** and is **kept up to date**?
- Is training **tailored** to particular roles?
- How do you assess the **effectiveness** of your training on topics related to financial crime?
- Is training material relevant and up to date? When was it **last reviewed**?

Examples of good practice	Examples of poor practice
•	•
• Staff in higher risk roles are subject to **more thorough vetting**.	• Staff are **not competent** to carry out preventative functions effectively, exposing the firm to financial crime risk.
• **Temporary staff** in higher risk roles are subject to the same level of vetting as permanent members of staff in similar roles.	• Staff vetting is a **one-off** exercise.
• Where **employment agencies** are used, the firm periodically satisfies itself that the agency is adhering to the agreed vetting standard.	• The firm fails to **identify changes** that could affect an individual's integrity and suitability.
• **Tailored** training is in place to ensure staff knowledge is adequate and up to date.	• The firm **limits enhanced vetting** to senior management roles and fails to vet staff whose roles expose them to higher financial crime risk.

Examples of good practice	Examples of poor practice
• New staff in **customer-facing** positions receive financial crime training tailored to their role before being able to interact with customers.	• The firm fails to identify whether staff whose roles expose them to bribery and corruption risk have **links to relevant political or administrative decision-makers**.
• Training has a strong **practical** dimension (e.g. case studies) and some form of testing.	• Poor compliance records are not reflected in **staff appraisals and remuneration**.
• The firm satisfies itself that staff **understand** their responsibilities (e.g. computerised training contains a test).	• Training dwells unduly on **legislation and regulations** rather than practical examples.
• **Whistleblowing** procedures are clear and accessible, and respect staff confidentiality.	• Training material is **not kept up to date**.
	• The firm **fails to identify** training needs.
	• There are no **training logs** or tracking of employees' training history.
	• Training **content** lacks management sign-off.
	• Training does not cover **whistleblowing** and **escalation** procedures.

See SYSC 3.1.6R and SYSC 5.1.1R.

Quality of oversight

2.2.7 G A firm's efforts to combat financial crime should be subject to **challenge**. We expect senior management to ensure that policies and procedures are appropriate and followed.

Self-assessment questions:

- How does your firm ensure that its approach to reviewing the effectiveness of financial crime systems controls is **comprehensive**?
- What are the **findings** of recent internal audits and compliance reviews on topics related to financial crime?
- How has the firm progressed **remedial measures**?

Examples of good practice	Examples of poor practice
• **Internal audit** and **compliance** routinely test the firm's defences against financial crime, including specific financial crime threats.	• Compliance unit and audit teams **lack experience** in financial crime matters.

Examples of good practice	Examples of poor practice
• Decisions on allocation of compliance and audit resource are **risk-based**. • Management **engage constructively** with processes of oversight and challenge. • Smaller firms seek **external help** if needed.	• Audit findings and compliance conclusions are **not shared** between business units. Lessons are not spread more widely.

2.3 Further guidance

2.3.1 G *FCTR* contains the following additional guidance on governance:

- FCTR 6.3.1G (Governance), from the *FSA's* thematic review Data security in Financial Services
- FCTR 8.3.1G (Senior management responsibility) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 9.3.1G (Governance and management information) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking
- FCTR 11.3.1G (Governance, culture and information sharing) from the *FSA's* thematic review Mortgage fraud against lenders

2.3.2 G *FCTR* contains the following additional guidance on **risk assessment**:

- FCTR 8.3.2G (Risk assessment) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 9.3.2G (Risk assessment and responses to significant bribery and corruption events) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking
- FCTR 10.3.7G (Responsibilities and risk assessments) from the *FSA's* thematic review The Small Firms Financial Crime Review
- FCTR 12.3.3G (High risk customers and PEPs – Risk assessment) and (Correspondent banking – Risk assessment of respondent banks) from the *FSA's* thematic review Banks' management of high money laundering risk situations

2.3.3 G *FCTR* contains the following additional guidance on **policies and procedures**:

- FCTR 8.3.3G (Policies and procedures) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 10.3.1G (Regulatory/Legal obligations) from the *FSA's* thematic review The Small Firms Financial Crime Review

- ■ FCTR 12.3.2G (High risk customers and PEPs – AML policies and procedures) from the *FSA's* thematic review Banks' management of high money laundering risk situations

2.3.4 G *FCTR* contains the following additional guidance on **staff recruitment, vetting, training and awareness**:

- ■ FCTR 6.3.2G (Training and awareness) and ■ FCTR 6.3.3G (Staff recruitment and vetting) from the *FSA's* thematic review Data security in Financial Services

- ■ FCTR 8.3.4G (Staff training and awareness) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions

- ■ FCTR 9.3.5G (Staff recruitment and vetting) and ■ FCTR 9.3.6G (Training and awareness) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking

- ■ FCTR 10.3.6G (Training) from the *FSA's* thematic review The Small Firms Financial Crime Review

- ■ FCTR 11.3.6G (Staff recruitment and vetting) and ■ FCTR 11.3.8G (Staff training and awareness) from the *FSA's* thematic review Mortgage fraud against lenders laundering risk situations

2.3.5 G *FCTR* contains the following additional guidance on **quality of oversight**:

- ■ FCTR 6.3.15G (Internal audit and compliance monitoring) from the *FSA's* thematic review Data security in Financial Services

- ■ FCTR 9.3.9G (The role of compliance and internal audit) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking

- ■ FCTR 11.3.5G (Compliance and internal audit) from the *FSA's* thematic review Mortgage fraud against lenders

2.3.6 G For firms' obligations in relation to whistleblowers see the Public Interest Disclosure Act 1998: www.legislation.gov.uk/ukpga/1998/23/contents