Financial Conduct Authority

Financial crime: a guide for firms

Part 2: Financial crime thematic reviews

March 2016

Contents

1. Introduction

1.1 Part 2 of *Financial crime: a guide for firms* contains summaries of, and links to, thematic reviews of various financial crime risks. It includes the consolidated examples of good and poor practice that were included with the reviews' findings. Each chapter includes a statement about those to whom it is most relevant and, where good and poor practice is included, to whom that guidance applies. We have suggested where material may be of interest and use to a broader range of firms, but we will only take guidance as applying to those types of firms to whom we have directly applied it. Each chapter also includes cross references to relevant chapters in Part 1.

1.2 The statements of our expectations and the examples of good and poor practice in the body of Part 2 have the same status as in Part 1: they are "general guidance" as defined by section 158 of the Financial Services and Markets Act 2000. The guidance in Part 2 is not binding and imposes no requirements on firms. Please refer to Chapter 1 of Part 1 for more information about guidance in the Guide.

1.3 As with Part 1, Part 2 contains guidance on Handbook rules and principles, particularly:

- SYSC 3.2.6R and SYSC 6.1.1R, which require firms to establish and maintain effective systems and controls to prevent the risk that they might be used to further financial crime;
- Principles 1 (integrity), 2 (skill, care and diligence), 3 (management and control) and 11 (relations with regulators) of our Principles for Businesses, which are set out in PRIN 2.1.1R;
- the Statements of Principle for Approved Persons set out in APER 2.1A.3R and the conduct rules in COCON 2.1 and 2.2; and
- in relation to guidance on money laundering, the rules in SYSC 3.2.6AR to SYSC 3.2.6JG and SYSC 6.3 (Financial crime).

Chapters 4, 5, and 12 also contain guidance on how firms can meet the requirements of the Money Laundering Regulations 2007; Chapter 12 also contains guidance on the EU Wire Transfer Regulation.[1]

1.4 Not all thematic reviews contain consolidated examples of good and poor practice. All reports do, however, discuss what the *FSA* found about the practices in place at the firms it visited. This information is not guidance, but firms interested in comparing themselves against their peers' systems and controls and policies and procedures in the areas covered by the reviews can find more information on this in the original reports.

1 EU Regulation 1781/2006 on information on the payer. See Part 1 Annex 1 of common terms for more information.

2.
Firms' high-level management of fraud risk (2006)

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

2.1 In February 2006 the *FSA* reviewed a sample of 16 firms (predominantly larger financial services groups) to assess how firms' senior management were managing fraud risk.

2.2 The findings of the review reflected our overall expectation that firms' senior management should be proactive in taking responsibility for identifying and assessing fraud risk and the adequacy of existing controls, and ensure that, if necessary, appropriate additional controls are put in place. We expect a firm to consider the full implications of the fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

2.3 The report emphasised that fraud is more than just a financial crime issue for firms; it is also a reputational one for the industry as a whole. The report concluded that while there had been some improvement in the management of fraud there was still more that firms could be doing to ensure fraud risk was managed effectively.

2.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 4 (Fraud) of Part 1 of this Guide.

The FSA's findings

2.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf

Consolidated examples of good and poor practice

2.6 This report did not contain consolidated examples of good and poor practice.

3.
Review of private banks' anti-money laundering systems and controls (2007)

Who should read this chapter? This chapter is relevant to **private banks** (firms which provide banking and investment services in a closely managed relationship to high net-worth clients) and **other firms conducting business with customers, such as PEPs, who might pose a higher risk of money laundering**. It may also be of interest to other firms we supervise under the Money Laundering Regulations 2007.

3.1 In July 2007 the *FSA* undertook a review of the anti-money laundering (AML) systems and controls at several *FSA*-regulated private banks. The review was conducted in response to a report by the *FSA's* Intelligence team, which had highlighted the high risk of money laundering within private banking.

3.2 This sector is particularly susceptible to money laundering and firms are expected to have high-standard AML systems and controls in place in order to mitigate these risks. The review focused on firms' policies and procedures for identifying, assessing, monitoring and managing the risks with a strong focus on high-risk clients and Politically Exposed Persons (PEPs).

3.3 The key areas examined in depth were a consideration of senior managements' risk appetite and the level of customer due diligence that took place.

3.4 Overall the *FSA* found that the private banks covered by our review acknowledged the relatively high risk of money laundering within their business activities and recognised the need to develop and implement strong AML systems and controls. The report also emphasised that private banks should obtain and keep up-to-date information on clients.

3.5 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

The FSA's findings

3.6 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf

Consolidated examples of good and poor practice

3.7 This report did not contain consolidated examples of good and poor practice.

4.
Automated Anti-Money Laundering Transaction Monitoring Systems (2007)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **all firms** for whom we are the supervisory authority under the Money Laundering Regulations 2007.

The extent to which we expect a firm to use automated anti-money laundering transaction monitoring (AML TM) systems depends on considerations such as the nature and scale of its business activities. There may be firms, particularly, **smaller firms**, that monitor credibly and effectively using manual procedures. This chapter will not apply to such firms where they do not, and are not intending to, use AML TM systems, although it may still be of interest to them.

4.1 The *FSA* wrote a short report on automated Anti-Money Laundering Transaction Monitoring Systems in July 2007. This was in anticipation of the fact that transaction monitoring would become compulsory following the implementation of the Money Laundering Regulations 2007.

4.2 The report explains that the *FSA* did not anticipate that there would be major changes in firms' practice, as the new framework expressed in law what firms were already doing. Instead, it is to be read as feedback on good practice to assist firms in complying with the Money Laundering Regulations 2007.

4.3 The report confirms our expectation that senior management should be in a position to monitor the performance of transaction monitoring (TM) systems, particularly at firms that experience operational or performance issues with their systems, to ensure issues are resolved in a timely fashion. Particular examples of good practice include transaction monitoring and profiling; especially ensuring unusual patterns of customer activity are identified.

4.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

The FSA's findings

4.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/money_laundering/aml_system.pdf

Consolidated examples of good and poor practice

This report contained the following Examples of good practice:

Box 4.1: Statement of good practice
• Depending on the nature and scale of a firm's business activities, automated AML TM systems may be an important component of an effective overall AML control environment.
Methodologies
• TM systems use profiling and/or rules-based monitoring methods.
• Profiling identifies unusual patterns of customer activity by applying statistical modelling techniques. These compare current patterns of activity to historical activity for that customer or peer group.
• Rules-based monitoring compares customer activity to fixed pre-set thresholds or patterns to determine if it is unusual.
Development and implementation
• A clear understanding of what the system will deliver and what constraints will be imposed by the limitations of the available data (including any issues arising from data cleanliness or legacy systems).
• Consideration of whether the vendor has the skills, resources and ability to deliver the promised service and provide adequate ongoing support.
• Maintenance of good working relations with the vendor, e.g. when collaborating to agree detailed system configuration.
• Use of recommended hardware, not necessarily a firm's own standard, to reduce processing problems, or otherwise finding a solution that is a good fit with a firm's existing infrastructure.
• A full understanding of the data being entered into the system and of the business's requirements.
• Regular housekeeping and database maintenance (operational resilience is vital to ensure that queries do not back up).
• Careful consideration of the risks of commissioning a bespoke vendor system, which may be incompatible with future standard product upgrades.
• Continued allocation of sufficient resources to ensure manual internal suspicion reporting is effective, as TM can supplement, but not replace, human awareness in day-to-day business.
Effectiveness
• Analyse system performance at a sufficiently detailed level, for example on a rule-by-rule basis, to understand the real underlying drivers of the performance results.
• Set systems so they do not generate fewer alerts simply to improve performance statistics. There is a risk of 'artificially' increasing the proportion of alerts that are ultimately reported as suspicious activity reports without generating an improvement in the quality and quantity of the alerts being generated.
• Deploy analytical tools to identify suspicious activity that is currently not being flagged by existing rules or profile-based monitoring.

Box 4.1: Statement of good practice
• Allocate adequate resources to analysing and assessing system performance, in particular to define how success is measured and produce robust objective data to analyse performance against these measures.
• Consistently monitor from one period to another, rather than on an intermittent basis, to ensure that performance data is not distorted by, for example, ad hoc decisions to run particular rules at different times.
• Measure performance as far as possible against like-for-like comparators, e.g. peers operating in similar markets and using similar profiling and rules.
Oversight
• Senior management should be in a position to monitor the performance of TM systems, particularly at firms that are experiencing operational or performance issues with their systems, so that issues are resolved in a timely fashion.
• Close involvement of the project management process by major business unit stakeholders and IT departments is an important component of successful system implementation.
Reporting & review
• There should be a clear allocation of responsibilities for reviewing, investigating and reporting details of alerts generated by TM systems. Those responsible for this work should have appropriate levels of skill and be subject to effective operational control and quality assurance processes.

5.
Review of firms' implementation of a risk-based approach to anti-money laundering (AML) (2008)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **all firms** for whom we are the supervisory authority under the **Money Laundering Regulations 2007**.

5.1 In March 2008 the *FSA* conducted a review of firms' implementation of a risk-based approach to anti-money laundering. This followed the move to a more principles-based regulatory strategy from August 2006, when we replaced the detailed rules contained in the Money Laundering sourcebook with high-level rules in the Senior Management Arrangements, Systems and Controls sourcebook (SYSC) of the Handbook.

5.2 The *FSA* visited 43 firms in total and gathered additional information from approximately 90 small firms with a survey. The report explored in depth a number of key areas that required improvement, including a review of staff training and the need to ensure staff are aware that it is a constant requirement to ensure AML policies and procedures are up to date and effective.

5.3 Due to the wide range of firms the *FSA* visited, there were a number of different findings. There were many examples of good practice, particularly in the way the larger firms had fully embraced the risk- based approach to AML and senior management's accountability for effective AML. The *FSA* also recognised that smaller firms, which generally represent lower risk, had fewer resources to devote to money laundering risk assessment and mitigation.

5.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

The FSA's findings

5.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/jmlsg_guidance.pdf

Consolidated examples of good and poor practice

Box 5.1: Firms' implementation of a risk-based approach to AML

Examples of good practice:

- One large firm's procedures required it to undertake periodic Know Your Customer (KYC)/Customer Due Diligence (CDD) reviews of existing clients. The depth of the review is determined by the risk ranking assigned to the client. Clients rated A and B are reviewed every three years; Cs every two years; and Ds and Es are reviewed annually. For lower risk (A–C) clients, the review may amount to no more than refreshing the client's file to take account of: significant changes in ownership or capitalisation; changes in the client's line of business; addition of a Politically Exposed Person (PEP) to shareholders or senior management; or any negative news on the client's owners or senior managers. For high risk (D or E) clients, visits to the client are necessary to provide an extra layer of comfort. Such visits would typically cover: review of client's client take-on procedures; sample testing of KYC documentation on underlying clients; and, obtaining answers to outstanding queries on, e.g., annual AML certification, transaction queries, and potential PEP or sanctions hits.
- One building society undertook a comprehensive policy review following the publication of the 2006 JMLSG[2] guidance, in order to identify which parts of the business were affected and what action was needed. It identified eight core business areas, which represented the key operational areas exposed to risk from money laundering. These business areas were ranked in order of risk and formed into workstreams. The local managers from each workstream business area were then trained by the Compliance Policy

Examples of poor practice:

- Some firms did not have a robust approach to classifying the money laundering risk associated with their clients. For example, one wholesale small firm classified all its clients as low or medium risk, despite the fact that most of them were based in Eastern Europe, North Africa and the Middle East. Another firm's risk-assessment procedures provided that the Compliance Officer or MLRO[3] would determine the risk category for each client and would record the basis of the assessment for each client. However, a file review showed no evidence that risk assessments had actually been carried out.
- Some small firms had produced inadequate annual MLRO reports, which failed to demonstrate to their governing body and senior management that the firms' AML systems and controls were operating effectively. In one case, the MLRO stated categorically that there had been no perceived deficiencies in the suspicious activity reporting process. However, he was unable even to describe that process to us, so it was highly unlikely that he had ever reviewed the SAR[4] process for possible deficiencies.
- In one small firm, the MLRO was clearly not fully engaged in his role. For example, he was unaware that we had removed the Money Laundering sourcebook and he was still using an outdated (2003) edition of the JMLSG Guidance. It was not entirely clear whether this arose from a lack of interest in his MLRO function or from inadequate compliance resources at the firm, which left him with insufficient time to keep up to date with AML matters, or a combination of both.

2 Joint Money Laundering Steering Group. See Part 1 Annex 1 for common term
3 Joint Money Laundering Steering Group. See Part 1 Annex 1 for common term
4 Suspicious Activity Report. See Part 1 Annex 1 for common terms.

Box 5.1: Firms' implementation of a risk-based approach to AML

Examples of good practice

Team, using a series of presentations and individual workshops, to understand the impact of the risk-based approach, their individual responsibilities and the appropriate customer due diligence policies. These managers were then required to apply this awareness and their existing knowledge of their workstreams' business activities to create documented risk profiles covering customers, products, delivery channels and geography. The risk profiles were graded as Red, Amber and Green and customer due diligence and monitoring requirements set at appropriate levels.

- In response to the SYSC changes, one major bank decided to appoint the MLRO's line manager as the designated director with overarching responsibility for AML controls. This director was seen as the obvious choice for the role, given that his portfolio of responsibilities included fraud, risk and money laundering. The bank's decision formally to appoint a Board-level senior manager to this position was viewed as reinforcing the importance of having in place a robust AML control framework. Following his appointment, the director decided that the management information (MI) on AML issues he had hitherto received was too ad hoc and fragmented. So the SYSC/JMLSG changes proved to be a catalyst for the bank establishing more organised MI and a Group-level Financial Risk Committee to consider relevant issues. (In the past, various Risk Committees had considered such issues.) The new Committee's remit covered fraud, money laundering and sanctions issues; however, its primary focus was AML.

Examples of poor practice

- We found some cases of medium-sized and smaller firms documenting their client take-on procedures but not regularly updating those procedures and not always following them. For example, one firm told us that CDD information on clients was refreshed every time clients applied for a new product or service. However, a file review showed no evidence that this had been done.
- A number of medium-sized and small firms were unaware that it was illegal for them to deal with individuals or entities named on the Treasury's Financial Sanctions list. As a result, no screening of clients or transactions was being undertaken against that list.
- One firm said that it did not routinely check the Financial Sanctions list, because it did not deal with the type of client who might appear on the list.
- Some medium-sized and small firms admitted that staff AML training was an area where improvement was needed. One firm told us that training was delivered as part of an induction programme but not refreshed at regular intervals throughout the employee's career. Another firm said that it provided AML induction training only if a new joiner specifically requested it and no new employee had actually made such a request. The firm's MLRO took the view that most new employees came from the regulated sector, so should already be aware of their AML obligations. Such employees were merely required to sign a form to confirm that they were aware of the firm's AML procedures, but their understanding was never tested.

Box 5.1: Firms' implementation of a risk-based approach to AML

Examples of good practice:

- One large bank judged that staff AML training and awareness were suitable for the development of a risk-based approach. It saw a need to differentiate between AML requirements in various business units, so that training could be adapted to the needs of the job. So in Retail, training had been re-designed to produce a more balanced package. Accordingly, staff were required to undertake one training module per quarter, with the emphasis on a different area in each module and a test taken every quarter. The aim was to see what impact this constant 'drip feed' of training had on suspicious activity reporting. At the time of the *FSA's* visit, this bank was also in the throes of merging its anti-fraud and AML training. The overall objective was to make it more difficult for criminals to do business with the bank undetected.

6.
Data security in Financial Services (2008)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **all firms** subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R and to **e-money institutions** and **payment institutions** within our supervisory scope.

Content: This chapter contains sections on:

6.1 In April 2008 the *FSA* published the findings of our thematic review on how financial services firms in the UK were addressing the risk that customer data may be lost or stolen and used to commit fraud or other financial crime. The *FSA* visited 39 firms, including retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. The *FSA* also took into account our experience of data loss incidents dealt with by our Financial Crime Operations Team: during 2007, the team dealt with 56 cases of lost or stolen data from financial services firms.

6.2 The *FSA* found a wide variation between good practices demonstrated by firms that were committed to ensuring data security and weakness in firms that were not taking adequate steps. Overall, the *FSA* found that data security in financial services firms needed to be improved significantly.

6.3 The report concluded that poor data security was a serious, widespread and high-impact risk, and that firms were often failing to consider the wider risks of identity fraud which could occur from cases of significant data loss and the impact of this on consumers. The *FSA* found that firms lacked a clear understanding of these risks and were therefore failing properly to inform customers, resulting in a lack of transparency.

6.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 5 (Data security) of Part 1 of this Guide.

The FSA's findings

6.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/data_security.pdf

Consolidated examples of good and poor practice

Box 6.1: Governance

Examples of good practice	Examples of poor practice
• Identification of data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment. • A senior manager with overall responsibility for data security, specifically mandated to manage data security risk assessment and communication between the key stakeholders within the firm such as: senior management, information security, Human Resources, financial crime, security, IT, compliance and internal audit. • A specific committee with representation from relevant business areas to assess, monitor and control data security risk, which reports to the firm's Board. As well as ensuring coordinated risk management, this structure sends a clear message to all staff about the importance of data security. • Written data security policies and procedures that are proportionate, accurate and relevant to staff's day-to-day work. • An open and honest culture of communication with pre-determined reporting mechanisms that make it easy for all staff and third parties to report data security concerns and data loss without fear of blame or recrimination.	• Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process. • No written policies and procedures on data security. • Firms do not understand the need for knowledge-sharing on data security. • Failing to take opportunities to share information with, and learn from, peers and others about data security risk and not recognising the need to do so. • A 'blame culture' that discourages staff from reporting data security concerns and data losses. • Failure to notify customers affected by data loss in case the details are picked up by the media.

Box 6.1: Governance

Examples of good practice

- Firms seeking external assistance if they feel they do not have the necessary expertise to complete a data security risk assessment themselves.
- Firms liaising with peers and others to increase their awareness of data security risk and the implementation of good systems and controls.
- Detailed plans for reacting to a data loss including when and how to communicate with affected customers.
- Firms writing to affected customers promptly after a data loss, telling them what has been lost and how it was lost.
- Firms offering advice on protective measures against identity fraud to consumers affected by data loss and, where appropriate, paying for such services to be put in place.

Box 6.2: Training and awareness

Examples of good practice

- Innovative training and awareness campaigns that focus on the financial crime risks arising from poor data security, as well as the legal and regulatory requirements to protect customer data.
- Clear understanding among staff about why data security is relevant to their work and what they must do to comply with relevant policies and procedures.
- Simple, memorable and easily digestible guidance for staff on good data security practice.
- Testing of staff understanding of data security policies on induction and once a year after that.
- Competitions, posters, screensavers and group discussion to raise interest in the subject.

Examples of poor practice

- No training to communicate policies and procedures.
- Managers assuming that employees understand data security risk without any training.
- Data security policies which are very lengthy, complicated and difficult to read.
- Reliance on staff signing an annual declaration stating that they have read policy documents without any further testing.
- Staff being given no incentive to learn about data security.

Box 6.3: Staff recruitment and vetting

Examples of good practice	Examples of poor practice
• Vetting staff on a risk-based approach, taking into account data security and other fraud risk. • Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists and the CIFAS Staff Fraud Database – for staff in roles with access to large amounts of customer data. • Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process. • A good understanding of vetting conducted by employment agencies for temporary and contract staff. • Formalised procedures to assess regularly whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.	• Allowing new recruits to access customer data before vetting has been completed. • Temporary staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles. • Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

Box 6.4: Controls – access rights

Examples of good practice	Examples of poor practice
• Specific IT access profiles for each role in the firm, which set out exactly what level of IT access is required for an individual to do their job. • If a staff member changes roles or responsibilities, all IT access rights are deleted from the system and the user is set up using the same process as if they were a new joiner at the firm. The complexity of this process is significantly reduced if role-based IT access profiles are in place – the old one can simply be replaced with the new. • A clearly defined process to notify IT of forthcoming staff departures in order that IT accesses can be permanently disabled or deleted on a timely and accurate basis. • Regular reviews of staff IT access rights to ensure that there are no anomalies. • 'Least privilege' access to call recordings and copies of scanned documents obtained for 'know your customer' purposes.	• Staff having access to customer data that they do not require to do their job. • User access rights set up on a case-by-case basis with no independent check that they are appropriate. • Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals. • User accounts being left 'live' or only suspended (i.e. not permanently disabled) when a staff member leaves. • A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.

Box 6.4: Controls – access rights

Examples of good practice

- Authentication of customers' identities using, for example, touch-tone telephone before a conversation with a call centre adviser takes place. This limits the amount of personal information and/or passwords contained in call recordings.
- Masking credit card, bank account details and other sensitive data like customer passwords where this would not affect employees' ability to do their job.

Box 6.5: Controls – passwords and user accounts

Examples of good practice

- Individual user accounts – requiring passwords – in place for all systems containing customer data.
- Password standards at least equivalent to those recommended by Get Safe Online – a government-backed campaign group. In July 2011, their recommended standard for passwords was a combination of letters, numbers and keyboard symbols at least eight characters in length and changed regularly.
- Measures to ensure passwords are robust. These might include controls to ensure that passwords can only be set in accordance with policy and the use of password-cracking software on a risk-based approach.
- 'Straight-through processing', but only if complemented by accurate role-based access profiles and strong passwords.

Examples of poor practice

- The same user account and password used by multiple users to access particular systems.
- Names and dictionary words used as passwords.
- Systems that allow passwords to be set which do not comply with password policy.
- Individuals share passwords.

Box 6.6: Controls – monitoring access to customer data

Examples of good practice	Examples of poor practice
• Risk-based, proactive monitoring of staff's access to customer data to ensure it is being accessed and/or updated for a genuine business reason. • The use of software designed to spot suspicious activity by employees with access to customer data. Such software may not be useful in its 'off-the-shelf' format so it is good practice for firms to ensure that it is tailored to their business profile. • Strict controls over superusers' access to customer data and independent checks of their work to ensure they have not accessed, manipulated or extracted data that was not required for a particular task.	• Assuming that vetted staff with appropriate access rights will always act appropriately. Staff can breach procedures, for example by looking at account information relating to celebrities, be tempted to commit fraud themselves or be bribed or threatened to give customer data to criminals. • Names and dictionary words used as passwords. • Failing to monitor superusers or other employees with access to large amounts of customer data.

Box 6.7: Controls – data back-up

Examples of good practice	Examples of poor practice
• Firms conducting a proper risk assessment of threats to data security arising from the data back-up process – from the point that back-up tapes are produced, through the transit process to the ultimate place of storage. • Firms encrypting backed-up data that is held off-site, including while in transit. • Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment. • Back-up data being transferred by secure Internet links. • Due diligence on third parties that handle backed-up customer data so the firm has a good understanding of how it is secured, exactly who has access to it and how staff with access to it are vetted. • Staff with responsibility for holding backed-up data off-site being given assistance to do so securely. For example, firms could offer to pay for a safe to be installed at the staff member's home. • Firms conducting spot checks to ensure that data held off-site is held in accordance with accepted policies and procedures.	• Firms failing to consider data security risk arising from the backing up of customer data. • A lack of clear and consistent procedures for backing up data, resulting in data being backed up in several different ways at different times. This makes it difficult for firms to keep track of copies of their data. • Unrestricted access to back-up tapes for large numbers of staff at third party firms. • Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.

Box 6.8: Controls – access to the Internet and email

Examples of good practice	Examples of poor practice
• Giving Internet and email access only to staff with a genuine business need. • Considering the risk of data compromise when monitoring external email traffic, for example by looking for strings of numbers that might be credit card details. • Where proportionate, using specialist IT software to detect data leakage via email. • Completely blocking access to all Internet content which allows web-based communication. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software. • Firms that provide cyber-cafes for staff to use during breaks ensuring that web-based communications are blocked or that data cannot be transferred into the cyber-cafe, either in electronic or paper format.	• Allowing staff who handle customer data to have access to the Internet and email if there is no business reason for this. • Allowing access to web-based communication Internet sites. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software.

Box 6.9: Controls – key-logging devices

Examples of good practice	
• Regular sweeping for key-logging devices in parts of the firm where employees have access to large amounts of, or sensitive, customer data. (Firms will also wish to conduct sweeps in other sensitive areas. For example, where money can be transferred.) • Use of software to determine whether unusual or prohibited types of hardware have been attached to employees' computers. • Raising awareness of the risk of key-logging devices. The vigilance of staff is a useful method of defence. • Anti-spyware software and firewalls etc in place and kept up to date.	

Box 6.10: Controls – laptop

Examples of good practice	Examples of poor practice
• The encryption of laptops and other portable devices containing customer data.	• Unencrypted customer data on laptops.

Box 6.10: Controls – laptop

Examples of good practice	Examples of poor practice
• Controls that mitigate the risk of employees failing to follow policies and procedures. The *FSA* has dealt with several cases of lost or stolen laptops that arose from firms' staff not doing what they should. • Maintaining an accurate register of laptops issued to staff. • Regular audits of the contents of laptops to ensure that only staff who are authorised to hold customer data on their laptops are doing so and that this is for genuine business reasons. • The wiping of shared laptops' hard drives between uses.	• A poor understanding of which employees have been issued or are using laptops to hold customer data. • Shared laptops used by staff without being signed out or wiped between uses.

Box 6.11: Controls – portable media including USB devices and CDs

Examples of good practice	Examples of poor practice
• Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs. • Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted. • Maintaining an accurate register of staff allowed to use USB devices and staff who have been issued USB devices. • The use of software to prevent and/or detect individuals using personal USB devices. • Firms reviewing regularly and on a risk-based approach the copying of customer data to portable media to ensure there is a genuine business reason for it. • The automatic encryption of portable media attached to firms' computers. • Providing lockers for higher-risk staff such as call centre staff and superusers and restricting them from taking personal effects to their desks.	• Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media. • Failing to review regularly threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.

Box 6.12: Controls – physical security

Examples of good practice	Examples of poor practice
• Appropriately restricted access to areas where large amounts of customer data are accessible, such as server rooms, call centres and filing areas. • Using robust intruder deterrents such as keypad entry doors, alarm systems, grilles or barred windows, and closed circuit television (CCTV). • Robust procedures for logging visitors and ensuring adequate supervision of them while on site. • Training and awareness programmes for staff to ensure they are fully aware of more basic risks to customer data arising from poor physical security. • Employing security guards, cleaners etc directly to ensure an appropriate level of vetting and reduce risks that can arise through third–party suppliers accessing customer data. • Using electronic swipe card records to spot unusual behaviour or access to high risk areas. • Keeping filing cabinets locked during the day and leaving the key with a trusted member of staff. • An enforced clear-desk policy.	• Allowing staff or other persons with no genuine business need to access areas where customer data is held. • Failure to check electronic records showing who has accessed sensitive areas of the office. • Failure to lock away customer records and files when the office is left unattended.

Box 6.13: Controls – disposal of customer data

Examples of good practice	Examples of poor practice
• Procedures that result in the production of as little paper-based customer data as possible. • Treating all paper as 'confidential waste' to eliminate confusion among employees about which type of bin to use. • All customer data disposed of by employees securely, for example by using shredders (preferably cross-cut rather than straight-line shredders) or confidential waste bins. • Checking general waste bins for the accidental disposal of customer data. • Using a third-party supplier, preferably one with BSIA[5] accreditation, which provides a certificate of secure destruction, to shred or incinerate paper-based customer data. It is important for firms to have a good understanding of the supplier's process for destroying customer data and their employee vetting standards. • Providing guidance for travelling or home-based staff on the secure disposal of customer data. • Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon as they become obsolete.	• Poor awareness among staff about how to dispose of customer data securely. • Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed. • Staff working remotely failing to dispose of customer data securely. • Firms failing to provide guidance or assistance to remote workers who need to dispose of an obsolete home computer. • Firms stockpiling obsolete computers and other portable media for too long and in insecure environments. • Firms relying on others to erase or destroy their hard drives and other portable media securely without evidence that this has been done competently.

5 British Security Industry Association

Box 6.14: Managing third-party suppliers

Examples of good practice	Examples of poor practice
• Conducting due diligence of data security standards at third-party suppliers before contracts are agreed. • Regular reviews of third-party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified. • Ensuring third-party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data. • Only allowing third-party IT suppliers access to customer databases for specific tasks on a case-by-case basis. • Third-party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe. • The use of secure internet links to transfer data to third parties.	• Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed. • Firms not knowing exactly which third-party staff have access to their customer data. • Firms not knowing how third-party suppliers' staff have been vetted. • Allowing third-party staff unsupervised access to areas where customer data is held when they have not been vetted to the same standards as employees. • Allowing IT suppliers unrestricted or unmonitored access to customer data. • A lack of awareness of when/how third-party suppliers can access customer data and failure to monitor such access. • Unencrypted customer data being sent to third parties using unregistered post.

Box 6.15: Internal audit and compliance monitoring

Examples of good practice	Examples of poor practice
• Firms seeking external assistance where they do not have the necessary in-house expertise or resources. • Compliance and internal audit conducting specific reviews of data security which cover all relevant areas of the business including IT, security, HR, training and awareness, governance and third-party suppliers. • Firms using expertise from across the business to help with the more technical aspects of data security audits and compliance monitoring.	• Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures. • Compliance consultants adopting a 'one size fits all' approach to different clients' businesses.

7. Review of financial crime controls in offshore centres (2008)

Who should read this chapter? This chapter is relevant to:

- **all firms** subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R; and
- **e-money institutions** and **payment institutions** within our supervisory scope who have or are considering establishing operations in offshore centres.

7.1 In the second half of 2008 the *FSA* reviewed how financial services firms in the UK were addressing financial crime risks in functions they had moved to offshore centres. The review followed on from the *FSA's* report into data security in financial services (April 2008 – http://www.fsa.gov.uk/pubs/other/data_security.pdf).

7.2 The main financial crime risks the *FSA* reviewed were: customer data being lost or stolen and used to facilitate fraud; money laundering; and fraud. The review found that, while there were good data security controls in place across the industry, continued effort was required to ensure controls did not break down and that they remained 'valid and risk-based'.

7.3 The review emphasised the importance of appropriate vetting and training of all staff, particularly with regard to local staff who had financial crime responsibilities. An examination revealed that training in this area was often lacking and not reflective of the needs of, and work done by, members of staff. The report emphasised that senior management should ensure that staff operating in these roles were given proper financial crime training as well as ensuring they possessed the appropriate technical know-how. The review also highlighted that, due to high staff turnover, firms needed appropriate and thorough vetting controls to supplement inadequate local electronic intelligence and search systems.

7.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 5 (Data security) of Part 1 of this Guide.

The FSA's findings

7.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pages/About/What/financial_crime/library/reports/review_offshore.shtml

Consolidated examples of good and poor practice

7.6 This report did not contain consolidated examples of good and poor practice.

8.
Financial services firms' approach to UK financial sanctions

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **all firms** subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R and to **e-money institutions** and **payment institutions** within our supervisory scope.

Content: This chapter contains sections on:

8.1 In April 2009 the *FSA* published the findings of our thematic review of firms' approach to UK financial sanctions. The *FSA* received 228 responses to an initial survey from a broad range of firms across the financial services industry, ranging from small firms to major financial groups, both retail and wholesale. Tailored surveys were sent to different types of firms to ensure that the questions were relevant to the nature and scale of the business of each firm. The *FSA* then selected a sub-sample of 25 firms to visit to substantiate the findings from the surveys.

8.2 The review highlighted areas where there was significant scope across the industry for improvement in firms' systems and controls to comply with the UK financial sanctions regime. The *FSA* found that, while some firms had robust systems in place that were appropriate to their business need, others, including some major firms, lacked integral infrastructure and struggled with inappropriate systems for their business. In small firms in particular, the *FSA* found a widespread lack of awareness of the UK financial sanctions regime.

8.3 The report examined a number of key areas of concern which included an in-depth look at whether senior management were aware of their responsibilities and, if so, were responding in an appropriate manner. The *FSA* also identified issues over the implementation of policies and procedures, particularly those put in place to ensure that staff were adequately trained, were kept aware of changes in this area, and knew how to respond when sanctions were imposed. The *FSA* also had concerns about firms' screening of clients, both initially and as an ongoing process.

8.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 7 (Sanctions and asset freezes) of Part 1 of this Guide.

The FSA's findings

8.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/Sanctions_final_report.pdf

Consolidated examples of good and poor practice

Box 8.1: Senior management responsibility	
Examples of good practice	Examples of poor practice
• Senior management involvement in approving and taking responsibility for policies and procedures. • A level of senior management awareness of the firm's obligations regarding financial sanctions sufficient to enable them to discharge their functions effectively. • Appropriate escalation in cases where a potential target match cannot easily be verified. • Adequate and appropriate resources allocated by senior management. • Appropriate escalation of actual target matches and breaches of UK financial sanctions.	• No senior management involvement or understanding regarding the firm's obligations under the UK financial sanctions regime, or its systems and controls to comply with it. • No, or insufficient, management oversight of the day-to-day operation of systems and controls. • Failure to included assessments of the financial sanctions systems and controls as a normal part of internal audit programmes. • No senior management involvement in any cases where a potential target match cannot easily be verified. • Senior management never being made aware of a target match or breach of sanctions for an existing customer. • Failure to notify customers affected by data loss in case the details are picked up by the media.

Box 8.2: Risk assessment	
Examples of good practice	Examples of poor practice
• Conducting a comprehensive risk assessment, based on a good understanding of the financial sanctions regime, covering the risks that may be posed by clients, transactions, services, products and jurisdictions. • Taking into account associated parties, such as directors and beneficial owners. • A formal documented risk assessment with a clearly documented rationale for the approach.	• Not assessing the risks that the firm may face of breaching financial sanctions. • Risk assessments that are based on misconceptions.

Box 8.3: Policies and procedures

Examples of good practice	Examples of poor practice
• Documented policies and procedures in place, which clearly set out a firm's approach to complying with its legal and regulatory requirements in this area. • Group-wide policies for UK financial sanctions screening, to ensure that business unit-specific policies and procedures reflect the standard set out in group policy. • Effective procedures to screen against the Consolidated List[6] that are appropriate for the business, covering customers, transactions and services across all products and business lines. • Clear, simple and well understood escalation procedures to enable staff to raise financial sanctions concerns with management. • Regular review and update of policies and procedures. • Regular reviews of the effectiveness of policies, procedures, systems and controls by the firm's internal audit function or another independent party. • Procedures that include ongoing monitoring/screening of clients.	• No policies or procedures in place for complying with the legal and regulatory requirements of the UK financial sanctions regime. • Internal audits of procedures carried out by persons with responsibility for oversight of financial sanctions procedures, rather than an independent party.

Box 8.4: Staff training and awareness

Examples of good practice	Examples of poor practice
• Regularly updated training and awareness programmes that are relevant and appropriate for employees' particular roles. • Testing to ensure that employees have a good understanding of financial sanctions risks and procedures. • Ongoing monitoring of employees' work to ensure they understand the financial sanctions procedures and are adhering to them. • Training provided to each business unit covering both the group-wide and business unit-specific policies on financial sanctions.	• No training on financial sanctions. • Relevant staff unaware of the firm's policies and procedures to comply with the UK financial sanctions regime. • Changes to the financial sanctions policies, procedures, systems and controls are not communicated to relevant staff.

6 See Part 1 Annex 1 for descriptions of common term

Box 8.5: Screening during client take-on

Examples of good practice	Examples of poor practice
• An effective screening system appropriate to the nature, size and risk of the firm's business. • Screening against the Consolidated List at the time of client take-on before providing any services or undertaking any transactions for a customer. • Screening directors and beneficial owners of corporate customers. • Screening third party payees where adequate information is available. • Where the firm's procedures require dual control (e.g. a 'four eyes' check) to be used, having in place an effective process to ensure this happens. • The use of 'fuzzy matching' where automated screening systems are used. • Where a commercially available automated screening system is implemented, making sure that there is a full understanding of the capabilities and limits of the system.	• Screening only on notification of a claim on an insurance policy, rather than during client take-on. • Relying on other FSA-authorised firms and compliance consultants to screen clients against the Consolidated List without taking reasonable steps to ensure that they are doing so effectively. • Assuming that AML customer due diligence checks include screening against the Consolidated List. • Failing to screen UK-based clients on the assumption that there are no UK-based persons or entities on the Consolidated List or failure to screen due to any other misconception. • Large global institutions with millions of clients using manual screening, increasing the likelihood of human error and leading to matches being missed. • IT systems that cannot flag potential matches clearly and prominently. • Firms calibrating their screening rules too narrowly or too widely so that they, for example, match only exact names with the Consolidated List or generate large numbers of resource intensive false positives. • Regarding the implementation of a commercially available sanctions screening system as a panacea, with no further work required by the firm. • Failing to tailor a commercially available sanctions screening system to the firm's requirements.

Box 8.6: Ongoing screening

Examples of good practice	Examples of poor practice
• Screening of the entire client base within a reasonable time following updates to the Consolidated List. • Ensuring that customer data used for ongoing screening is up to date and correct.	• No ongoing screening of customer databases or transactions. • Failure to screen directors and beneficial owners of corporate customers and/ or third party payees where adequate information is available.

Box 8.6: Ongoing screening

Examples of good practice	Examples of poor practice
• Processes that include screening for indirect as well as direct customers and also third party payees, wherever possible. • Processes that include screening changes to corporate customers' data (e.g. when new directors are appointed or if there are changes to beneficial owners). • Regular reviews of the calibration and rules of automated systems to ensure they are operating effectively. • Screening systems calibrated in accordance with the firm's risk appetite, rather than the settings suggested by external software providers. • Systems calibrated to include 'fuzzy matching', including name reversal, digit rotation and character manipulation. • Flags on systems prominently and clearly identified. • Controls that require referral to relevant compliance staff prior to dealing with flagged individuals or entities.	• Failure to review the calibration and rules of automated systems, or to set the calibration in accordance with the firm's risk appetite. • Flags on systems that are dependent on staff looking for them. • Controls on systems that can be overridden without referral to compliance.

Box 8.7: Treatment of potential target matches

Examples of good practice	Examples of poor practice
• Procedures for investigating whether a potential match is an actual target match or a false positive. • Procedures for freezing accounts where an actual target match is identified. • Procedures for notifying the Treasury's AFU promptly of any confirmed matches. • Procedures for notifying senior management of target matches and cases where the firm cannot determine whether a potential match is the actual target on the Consolidated List. • A clear audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.	• No procedures in place for investigating potential matches with the Consolidated List. • Discounting actual target matches incorrectly as false positives due to insufficient investigation. • No audit trail of decisions where potential target matches are judged to be false positives.

9.
Anti-bribery and corruption in commercial insurance broking (2010)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to:

- **commercial insurance brokers** and **other firms** who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R; and
- **e-money institutions** and **payment institutions** within our supervisory scope.

Except that Box **9.3** and Box **9.4** only apply to those **firms or institutions who use third parties to win business**. It may also be of interest to other firms who are subject to SYSC 3.2.6R and SYSC 6.1.1R.

Content: This chapter contains sections on:

9.1 In May 2010 the *FSA* published the findings of our review into the way commercial insurance broker firms in the UK addressed the risks of becoming involved in corrupt practices such as bribery. The *FSA* visited 17 broker firms. Although this report focused on commercial insurance brokers, the findings are relevant in other sectors.

9.2 The report examined standards in managing the risk of illicit payments or inducements to, or on behalf of, third parties in order to obtain or retain business.

9.3 The report found that many firms' approach towards high-risk business was not of an acceptable standard and that there was a risk that firms were not able to demonstrate that adequate procedures were in place to prevent bribery from occurring.

9.4 The report identified a number of common concerns including weak governance and a poor understanding of bribery and corruption risks among senior managers as well as very little or no specific training and weak vetting of staff. The *FSA* found that there was a general failure to implement a risk-based approach to anti-bribery and corruption and very weak due diligence and monitoring of third-party relationships and payments.

9.5 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 6 (Bribery and corruption) of Part 1 of this Guide.

The FSA's findings

9.6 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/anti_bribery.pdf

Consolidated examples of good and poor practice

Box 9.1: Governance and management information

Examples of good practice	Examples of poor practice
• Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate Terms of Reference and senior management membership, reporting ultimately to the Board. • Good Board-level and senior management understanding of the bribery and corruption risks faced by the firm, the materiality to their business and how to apply a risk-based approach to anti-bribery and corruption work. • Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls. • Regular MI to the Board and other relevant senior management forums. • MI includes information about third parties including (but not limited to) new third party accounts, their risk classification, higher risk third party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties. • MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption. • Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.	• Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or appropriately formed committee. • A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level. • Little or no MI sent to the Board about higher-risk third-party relationships or payments. • Failing to include details of wider issues, such as new legislation or regulatory developments in MI. • IT systems unable to produce the necessary MI.

Box 9.2: Risk assessment and responses to significant bribery and corruption events

Examples of good practice

- Regular assessments of bribery and corruption risks with a specific senior person responsible for ensuring this is done, taking into account the country and class of business involved as well as other relevant factors.
- More robust due diligence on and monitoring of higher–risk third-party relationships.
- Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship.
- Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary.
- Establishing clear plans to implement improvements arising from reviews, including updating policies, procedures and staff training.
- Adequate and prompt reporting to SOCA[7] and us of any inappropriate payments identified during business practice review.

Examples of poor practice

- Failing to consider the bribery and corruption risks posed by third parties used to win business.
- Failing to allocate formal responsibility for anti-bribery and corruption risk assessments.
- A 'one size fits all' approach to third-party due diligence.
- Failing to respond to external events which may draw attention to weaknesses in systems and controls.
- Taking too long to implement changes to systems and controls after analysing external events.
- Failure to bolster insufficient in-house knowledge or resource with external expertise.
- Failure to report inappropriate payments to SOCA and a lack of openness in dealing with us concerning any material issues identified.

Box 9.3: Due diligence on third-party relationships

Examples of good practice

- Establishing and documenting policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third-party relationships.
- More robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for using them.
- Having a clear understanding of the roles clients, reinsurers, solicitors and loss adjusters play in transactions to ensure they are not carrying out higher-risk activities.
- Taking reasonable steps to verify the information provided by third parties during the due diligence process.

Examples of poor practice

- Failing to carry out or document due diligence on third-party relationships.
- Relying heavily on the informal 'market view' of the integrity of third parties as due diligence.
- Relying on the fact that third-party relationships are longstanding when no due diligence has ever been carried out.
- Carrying out only very basic identity checks as due diligence on higher-risk third-parties.
- Asking third parties to fill in account opening forms which are not relevant to them (e.g. individuals filling in forms aimed at corporate entities).
- Accepting vague explanations of the business case for using third parties.

7 Serious Organised Crime Agency. See Part 1 Annex 1 for common terms.

Box 9.3: Due diligence on third-party relationships

Examples of good practice

- Using third-party forms which ask relevant questions and clearly state which fields are mandatory.
- Having third-party account opening forms reviewed and approved by compliance, risk or committees involving these areas.
- Using commercially available intelligence tools, databases and/or other research techniques such as Internet search engines to check third-party declarations about connections to public officials, clients or the assured.
- Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission.
- Ensuring current third-party due diligence standards are appropriate when business is acquired that is higher risk than existing business.
- Considering the level of bribery and corruption risk posed by a third party when agreeing the level of commission.
- Setting 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.
- Paying commission to third parties on a one-off fee basis where their role is pure introduction.
- Taking reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque.
- Higher or extra levels of approval for high-risk third-party relationships.
- Regularly reviewing third-party relationships to identify the nature and risk profile of third-party relationships.
- Maintaining accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.

Examples of poor practice

- Approvers of third-party relationships working within the broking department or being too close to it to provide adequate challenge.
- Accepting instructions from third parties to pay commission to other individuals or entities which have not been subject to due diligence.
- Assuming that third-party relationships acquired from other firms have been subject to adequate due diligence.
- Paying high levels of commission to third parties used to obtain or retain higher risk business, especially if their only role is to introduce the business.
- Receiving bank details from third parties via informal channels such as email, particularly if email addresses are from webmail (e.g. Hotmail) accounts or do not appear to be obviously connected to the third party.
- Leaving redundant third-party accounts 'live' on the accounting systems because third-party relationships have not been regularly reviewed.
- Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.

Box 9.4: Payment controls

Examples of good practice

- Ensuring adequate due diligence and approval of third-party relationships before payments are made to the third party.
- Risk-based approval procedures for payments and a clear understanding of why payments are made.
- Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account.
- Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments.
- A healthily sceptical approach to approving third-party payments.
- Adequate due diligence on new suppliers being added to the Accounts Payable system.
- Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced.
- Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment.
- Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved.
- The facility to produce accurate MI to facilitate effective payment monitoring.

Examples of poor practice

- Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.
- The inability to produce regular third-party payment schedules for review.
- Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.
- No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.
- The giving or receipt of cash gifts.

Box 9.5: Staff recruitment and vetting

Examples of good practice

- Vetting staff on a risk-based approach, taking into account financial crime risk.
- Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially available intelligence databases and the CIFAS Staff Fraud Database – for staff in roles with higher bribery and corruption risk.
- A risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role.

Examples of poor practice

- Relying entirely on an individual's market reputation or market gossip as the basis for recruiting staff.
- Carrying out enhanced vetting only for senior staff when more junior staff are working in positions where they could be exposed to bribery or competition issues.
- Failing to consider on a continuing basis whether staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

Box 9.5: Staff recruitment and vetting

Examples of good practice	Examples of poor practice
• Where employment agencies are used to recruit staff in higher-risk positions, having a clear understanding of the checks they carry out on prospective staff. • Conducting periodic checks to ensure that agencies are complying with agreed vetting standards. • A formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in, or committing, corrupt practices.	• Relying on contracts with employment agencies covering staff vetting standards without checking periodically that the agency is adhering to them. • Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

Box 9.6: Training and awareness

Examples of good practice	Examples of poor practice
• Providing good quality, standard training on anti-bribery and corruption for all staff. • Additional anti-bribery and corruption training for staff in higher risk positions. • Ensuring staff responsible for training others have adequate training themselves. • Ensuring training covers practical examples of risk and how to comply with policies. • Testing staff understanding and using the results to assess individual training needs and the overall quality of the training. • Staff records setting out what training was completed and when. • Providing refresher training and ensuring it is kept up to date.	• Failing to provide training on anti-bribery and corruption, especially to staff in higher risk positions. • Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them. • Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff. • Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.

Box 9.7: Risk arising from remuneration structures

Examples of good practice	Examples of poor practice
• Assessing whether remuneration structures give rise to increased risk of bribery and corruption. • Determining individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated. • Deferral and clawback provisions for bonuses paid to staff in higher-risk positions.	• Bonus structures for staff in higher-risk positions which are directly linked (e.g. by a formula) solely to the amount of income or profit they produce, particularly when bonuses form a major part, or the majority, of total remuneration.

Box 9.8: Incident reporting

Examples of good practice	Examples of poor practice
• Clear procedures for whistleblowing and reporting suspicions, and communicating these to staff. • Appointing a senior manager to oversee the whistleblowing process and act as a point of contact if an individual has concerns about their line management. • Respect for the confidentiality of workers who raise concerns. • Internal and external suspicious activity reporting procedures in line with the Joint Money Laundering Steering Group guidance. • Keeping records or copies of internal suspicion reports which are not forwarded as SARs for future reference and possible trend analysis. • Financial crime training covers whistleblowing procedures and how to report suspicious activity.	• Failing to report suspicious activity relating to bribery and corruption. • No clear internal procedure for whistleblowing or reporting suspicions. • No alternative reporting routes for staff wishing to make a whistleblowing disclosure about their line management or senior managers. • A lack of training and awareness in relation to whistleblowing the reporting of suspicious activity.

Box 9.9: The role of compliance and internal audit

Examples of good practice	Examples of poor practice
• Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of bribery and corruption risks. • Effective compliance monitoring and internal audit reviews which challenge not only whether processes to mitigate bribery and corruption have been followed but also the effectiveness of the processes themselves. • Independent checking of compliance's operational role in approving third-party relationships and accounts, where relevant. • Routine compliance and/or internal audit checks of higher-risk third-party payments to ensure there is appropriate supporting documentation and adequate justification to pay.	• Failing to carry out compliance or internal audit work on anti-bribery and corruption. • Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts. • Compliance and internal audit not recognising or acting on the need for a risk-based approach.

10.
The Small Firms Financial Crime Review (2010)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **small firms** in all sectors who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R and small **e-money institutions** and **payment institutions** within our supervisory scope.

Content: This chapter contains sections on:

10.1 In May 2010 the *FSA* published the findings of its thematic review into the extent to which small firms across the financial services industry addressed financial crime risks in their business. The review conducted visits to 159 small retail and wholesale firms in a variety of financial sectors. It was the first systematic review of financial crime systems and controls in small firms conducted by the *FSA*.

10.2 The review covered three main areas: anti-money laundering and financial sanctions; data security; and fraud controls. The review sought to determine whether firms understood clearly

the requirements placed on them by the wide range of legislation and regulations to which they were subject.

10.3 The *FSA* found that firms generally demonstrated a reasonable awareness of their obligations, particularly regarding AML systems and controls. But it found weaknesses across the sector regarding the implementation of systems and controls put in place to reduce firms' broader financial crime risk.

10.4 The review emphasised the key role that the small firms sector often plays in acting as the first point of entry for customers to the wider UK financial services industry; and the importance, therefore, of firms having adequate customer due diligence measures in place. The report flagged up concerns relating to weaknesses in firms' enhanced due diligence procedures when dealing with high-risk customers.

10.5 The *FSA* concluded that, despite an increased awareness of the risks posed by financial crime and information supplied by the *FSA*, small firms were generally weak in their assessment and mitigation of financial crime risks.

10.6 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls), Chapter 3 (Money laundering and terrorist financing), Chapter 4 (Fraud), Chapter 5 (Data security) and Chapter 7 (sanctions and asset freezes) of Part 1 of this Guide.

The FSA's findings

10.7 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/smallfirms/pdf/financial_crime_report.pdf

Consolidated examples of good and poor practice

Box 10.1: Regulatory/legal obligations

Examples of good practice	Examples of poor practice
• A small IFA used policies and procedures which had been prepared by consultants but the MLRO had tailored these to the firm's business. There was also a risk assessment of customers and products included in an MLRO report which was updated regularly. • One general insurance (GI) intermediary had an AML policy in place which was of a very good standard and included many good examples of AML typologies relevant to GI business. Despite the fact that there is no requirement for an MLRO for a business of this type the firm had appointed an individual to carry out an MLRO function as a point of good practice.	• An MLRO at an IFA was not familiar with the JMLSG guidance and had an inadequate knowledge of the firm's financial crime policies and procedures.

Box 10.2: Account opening procedures

Examples of good practice	Examples of poor practice
• A discretionary portfolio manager had procedures that required the verification of the identity of all beneficial owners. The firm checked its customer base against sanctions lists and had considered the risks associated with PEPs. Most new customers were visited by the adviser at home and in these cases the advisers would usually ask for identity verification documents on the second meeting with the customer. Where business was conducted remotely, more (three or four) identity verification documents were required and the source of funds exemption was not used.	• An IFA commented that they only dealt with investment customers that were well known to the firm or regulated entities. However, the firm had some high risk customers who were subject to very basic due diligence (e.g. copy of passport). The firm said that they were concerned about the high reputational impact an AML incident could have on their small, young business. The firm stated that they would deal with PEPs but with appropriate care. However, the firm did not have a rigorous system in place to be able to identify PEPs – this was a concern given the nationality and residence of some underlying customers. The firm appeared to have reasonable awareness of the sanctions requirements of both the Treasury and the United States Office of Foreign Assets Control (OFAC), but there was no evidence in the customer files of any sanctions checking. • A venture capital firm had policies in place which required a higher level of due diligence and approval for high-risk customers. However, they had no system in place by which they could identify this type of customer.

Box 10.3: Monitoring activity

Examples of good practice	
• A credit union used a computer-based monitoring system which had been specially designed for business of this type. The system was able to produce a number of exception reports relating to the union's members, including frequency of transactions and defaulted payments. The exceptions reports were reviewed daily. If there had been no activity on an account for 12 months it was suspended. If the customer was to return and request a withdrawal they would be required to prove their identity again.	

Box 10.3: Monitoring activity

Examples of good practice

- A Personal Pension Operator's procedure for higher risk customers included gathering extra source of funds proof at customer take-on. The firm also conducted manual monitoring and produced valuation statements twice a year.
- Within a GI intermediary firm, there was a process where, if a customer made a quick claim after the policy has been taken out, their records were flagged on the firm's monitoring system. This acted as an alert for any possible suspicious claims in the future.

Box 10.4: Suspicious activity reporting

Examples of poor practice

- One MLRO working at an IFA firm commented that he would forward all internal SARs he received to SOCA and would not exercise any judgement himself as to the seriousness of these SARs.
- At an IFA the MLRO did not demonstrate any knowledge of how to report a SAR to SOCA, what to report to SOCA, or how to draft a SAR. The firm's policies and procedures contained a pro forma SAR but this was not a document the MLRO was familiar with.
- An IFA was unaware of the difference between reporting suspicions to SOCA and sanctions requirements, believing that if he identified a person on the Consolidated List he should carry on as normal and just report it as a SAR to SOCA.

Box 10.5: Records

Examples of good practice	Examples of poor practice
• An advising-only intermediary firm used a web-based system as its database of leads, contact names and addresses. It also stored telephone and meeting notes there which were accessed by staff using individual passwords. • A home finance broker classified customers as A, B or C for record keeping purposes. A's being Active, B's being 'one-off or infrequent business' who he maintained contact with via a regular newsletter and C's being archived customers.	• A file review at an IFA revealed disorganised files and missing KYC documentation in three of five files reviewed. Files did not always include a checklist (We expect that KYC information should be kept together in the file so that it is easily identifiable and auditable.)

Box 10.6: Training

Examples of good practice	Examples of poor practice
• A GI intermediary used an on-line training website (costing around £100 per employee per year). The firm believed that the training was good quality and included separate modules on financial crime which were compulsory for staff to complete. Staff were also required to complete refresher training. An audit of all training completed was stored on-line. • An IFA (sole trader) carried out on-line training on various financial crime topics. He also participated in conference call training where a trainer talked trainees through various topics while on-line; this was both time- and travel-efficient.	• A GI intermediary explained that the compliance manager carried out regular audits to confirm staff knowledge was sufficient. However, on inspection of the training files it appeared that training was largely limited to product information and customer service and did not sufficiently cover financial crime. • One credit union, apart from on-the-job training for new staff members, had no regular training in place and no method to test staff knowledge of financial crime issues.

Box 10.7: Responsibilities and risk assessments

Examples of good practice	Examples of poor practice
• At an IFA there was a clearly documented policy on data security which staff were tested on annually. The policy contained, but was not limited to, details around clear desks, non-sharing of passwords, the discouraging of the over-use of portable media devices, the secure disposal of data, and the logging of customer files removed and returned to the office.	• At an IFA, a risk assessment had been undertaken by the firm's compliance consultant but the firm demonstrated no real appreciation of the financial crime risks in its business. The risk assessment was not tailored to the risks inherent in that business.

Box 10.7: Responsibilities and risk assessments

Examples of good practice	Examples of poor practice
• An IFA had produced a written data security review of its business which had been prompted by their external consultants and largely followed the small firms' factsheet material on data security, provided by the *FSA* in April 2008. • In a personal pension operator, there was a full and comprehensive anti-fraud strategy in place and a full risk assessment had been carried out which was regularly reviewed. The firm's financial transactions were normally 'four-eyed' as a minimum and there were strict mandates on cheque signatures for the Finance Director and Finance Manager.	• An advising-only intermediary had its policies and procedures drawn up by an external consultant but these had not been tailored to the firm's business. The MLRO was unclear about investigating and reporting suspicious activity to SOCA. The firm's staff had not received formal training in AML or reporting suspicious activity to SOCA.

Box 10.8: Access to systems

Examples of good practice	Examples of poor practice
• In a Discretionary Investment Management firm, the Chief Executive ensured that he signed off on all data user profiles ensuring that systems accesses were authorised by him. • A discretionary investment manager conducted five-year referencing on new staff, verified personal addresses and obtained character references from acquaintances not selected by the candidate. They also carried out annual credit checks, CRB checks and open source Internet searches on staff. There were role profiles for each job within the firm and these were reviewed monthly for accuracy. • In a venture capital firm they imposed a minimum ten-character (alpha/numeric, upper/lower case) password for systems access which had a 45-day enforced change period.	• In a financial advisory firm there was no minimum length for passwords, (although these had to be alpha/numeric) and the principal of the firm plus one other colleague knew all staff members' passwords. • In an advising-only intermediary, staff set their own systems passwords which had no defined length or complexity and were only changed every six months.

Box 10.9: Outsourcing

Examples of good practice

- A discretionary investment manager used an external firm for IT support and had conducted its own on-site review of the IT firm's security arrangements. The same firm also insisted on CRB checks for cleaners.
- An IFA had received a request from an introducer to provide names of customers who had bought a certain financial product. The firm refused to provide the data as it considered the request unnecessary and wanted to protect its customer data. It also referred the matter to the Information Commissioner who supported the firm's actions.
- A general insurance intermediary employed office cleaners supplied by an agency that conducts due diligence including CRB checks. Office door codes were regularly changed and always if there was a change in staff.
- In an authorised professional firm, unauthorised data access attempts by staff were monitored by the IT manager and email alerts sent to staff and management when identified.
- In a general insurance intermediary the two directors had recently visited the offsite data storage facility to satisfy themselves about the security arrangements at the premises.

Examples of poor practice

- An authorised professional firm employed the services of third-party cleaners, security staff, and an offsite confidential waste company, but had carried out no due diligence on any of these parties.
- An IFA allowed a third-party IT consultant full access rights to its customer databank. Although the firm had a service agreement in place that allowed full audit rights between the advisor and the IT company to monitor the security arrangements put in place by the IT company, this had not been invoked by the IFA, in contrast to other firms visited where such audits had been undertaken.
- In an authorised professional firm, Internet and Hotmail usage was only monitored if it was for longer than 20 minutes at any one time. There was also no clear-desk policy within the firm.
- In an authorised professional firm there had been two incidents where people had walked into the office and stolen staff wallets and laptops.

Box 10.10: Physical controls

Examples of good practice

- At an IFA, staff email was monitored and monthly MI was produced, which included a monitoring of where emails had been directed to staff home addresses.
- At an investment advisory firm, staff were prohibited from using the Internet and Hotmail accounts. USB ports had been disabled on hardware and laptops were encrypted.

Examples of poor practice

- In a general insurance intermediary which had poor physical security in terms of shop front access, there were many insecure boxes of historical customer records dotted around the office in no apparent order. The firm had no control record of what was stored in the boxes, saying only that they were no longer needed for the business.

Box 10.11: Data disposal

Examples of good practice	Examples of poor practice
• An advising and arranging intermediary used a third party company for all paper disposals, using secure locked bins provided by the third party. All paper in the firm was treated as confidential and 'secure paper management' was encouraged throughout the firm, enhanced by a monitored clear-desk policy. The firm was also aware that it needed to consider a process for secure disposal of electronic media as it was due to undergo a systems refit in the near future. • An IFA treated all customer paperwork as confidential and had onsite shredding facilities. For bulk shredding the firm used a third party who provided bags and tags for labelling sensitive waste for removal, and this was collected and signed for by the third party. The firm's directors had visited the third party's premises and satisfied themselves of their processes. The directors periodically checked office bins for confidential waste being mishandled. PCs which had come to 'end of life' were wiped using reputable software and physically destroyed.	• In an IFA there was a clear-desk policy that was not enforced and customer data was stored in unlocked cabinets which were situated in a part of the office accessible to all visitors to the firm.

Box 10.12: Data compromise incidents

Examples of good practice	Examples of poor practice
• A general insurance broker had suffered a succession of break-ins to their offices. No data had been lost or stolen but the firm sought the advice of local police over the incidents and employed additional physical security as a result.	• In a general insurance intermediary, the IT manager said he would take responsibility for any data security incidents although there was no procedures in place for how to handle such occurrences. When asked about data security, the compliance officer was unable to articulate the financial crime risks that lax data security processes posed to the firm and said it would be something he would discuss with his IT manager.

Box 10.13: General fraud

Examples of good practice	Examples of poor practice
• A small product provider had assessed the fraud risk presented by each product and developed appropriate controls to mitigate this risk based on the assessment. This assessment was then set out in the firm's Compliance Manual and was updated when new information became available. • A credit union did not permit its members to change address details over the telephone. These needed to be submitted in writing/email. The firm also considered the feasibility of allocating passwords to their members for accessing their accounts. The union had photographs of all its members which were taken when the account was opened. These were then used to verify the identity of the customer should they wish to withdraw money or apply for a loan from the union. • One discretionary investment manager kept full records of all customer contact including details of any phone calls. When receiving incoming calls from product providers, the firm required the caller to verify where they were calling from and provide a contact telephone number which they were then called back on before any customer details were discussed or instructions taken. • One general insurance intermediary was a member of a local association whose membership included law enforcement and Law Society representatives. This group met in order to share local intelligence to help improve their firms' defences against financial crime.	• One GI broker permitted customers to contact the firm by telephone to inform the firm of any amendments to their personal details (including change of address). To verify the identity of the person they were speaking to, the firm asked security questions. However, all the information that the firm used to verify the customer's identity was available in the public domain.

Box 10.14: Insurance fraud

Examples of good practice	Examples of poor practice
• A small general insurer had compiled a handbook which detailed indicators of potential insurance fraud. • An IFA had undertaken a risk assessment to understand where his business was vulnerable to insurance fraud.	• An IFA had a procedure in place to aid in the identification of high-risk customers. However, once identified, this firm had no enhanced due diligence procedures in place to deal with such customers.

Box 10.14: Insurance fraud	
Examples of good practice • An IFA had identified where their business may be used to facilitate insurance fraud and implemented more controls in these areas.	

Box 10.15: Investment fraud	
Examples of good practice • An IFA had undertaken a risk assessment for all high-net-worth customers. • A discretionary investment manager referred higher-risk decisions (in respect of a high-risk customer/value of funds involved) to a specific senior manager. • A personal pension operator carried out a financial crime risk assessment for newly introduced investment products.	Examples of poor practice • An IFA had a 'one size fits all' approach to identifying the risks associated with customers and investments.

Box 10.16: Mortgage fraud	
Examples of good practice • The majority of firms conducted customer fact finds. This allowed them to know their customers sufficiently to identify any suspicious behaviour. CDD[8] (including source of funds information) was also obtained early in the application process before the application was completed and submitted to the lender. • A home finance broker would not conduct any remote business – meeting all customers face-to-face. • An IFA had informally assessed the mortgage fraud risks the business faced and was aware of potentially suspicious indicators. The IFA also looked at the fraud risks associated with how the company approached the firm – e.g. the firm felt that a cold call from a customer may pose a greater risk than those which had been referred by longstanding customers.	Examples of poor practice • An IFA did not undertake any KYC checks, considering this to be the responsibility of the lender. • An IFA did not investigate source of funds. The firm stated this was because 'a bank would pick it up and report it.' • An IFA did not undertake extra verification of its non-face-to-face customers.

8 Customer Due Diligence. See Part 1 Annex 1 for common terms.

Box 10.17: Staff/internal fraud

Examples of good practice	Examples of poor practice
• An IFA obtained full reference checks (proof of identity, eligibility to work and credit checks) prior to appointment. Original certificates or other original documentation was also requested. • An IFA ensured that staff vetting is repeated by completing a credit reference check on each member of staff. • An IFA set a low credit limit for each of its company credit cards. Bills are sent to the firm and each month the holder has to produce receipts to reconcile their claim. • At one authorised professional firm dual signatory requirements had to be met for all payments made over £5,000.	• One general insurance intermediary did not undertake any background checks before appointing a member of staff or authenticate qualifications or references. • Company credit card usage was not monitored or reconciled at an IFA. An IFA had the same computer log-on used by all staff in the office no matter what their role.

11.
Mortgage fraud against lenders (2011)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **mortgage lenders within our supervisory scope**. It may also be of interest to other firms who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R.

Content: This chapter contains sections on:

11.1 In June 2011 the *FSA* published the findings of its thematic review into how mortgage lenders in the UK were managing the risks mortgage fraud posed to their businesses. The project population of 20 banks and building societies was selected to be a representative sample of the mortgage lending market. The firms the *FSA* visited accounted for 56% of the mortgage market in 2010.

11.2 The *FSA's* review found the industry had made progress coming to terms with the problem of containing mortgage fraud over recent years. Defences were stronger, and the value of cross-industry cooperation was better recognised. However, the *FSA* found that many in the industry could do better; the *FSA* were disappointed, for example, that more firms were not actively participating in the *FSA's* Information From Lenders scheme and other industry-wide initiatives to tackle mortgage fraud. Other areas of concern the *FSA* identified were to do with the adequacy of firms' resources for dealing with mortgage fraud, both in terms of the number and experience of staff; and the *FSA* identified scope for significant improvement in the way lenders dealt with third parties such as brokers, valuers and conveyancers.

11.3 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 4 (Fraud) of Part 1 of this Guide.

The FSA's findings

11.4 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/mortgage_fraud.pdf

Consolidated examples of good and poor practice

Box 11.1: Governance, culture and information sharing

Examples of good practice	Examples of poor practice
• A firm's efforts to counter mortgage fraud are coordinated, and based on consideration of where anti-fraud resources can be allocated to best effect. • Senior management engage with mortgage fraud risks and receive sufficient management information about incidents and trends. • A firm engages in cross-industry efforts to exchange information about fraud risks. • A firm engages front-line business areas in anti-mortgage fraud initiatives.	• A firm fails to report relevant information to the Information From Lenders scheme as per the guidance on IFL referrals. • A firm fails to define mortgage fraud clearly, undermining efforts to compile statistics related to mortgage fraud trends. • A firm does not allocate responsibility for countering mortgage fraud clearly within the management hierarchy.

Box 11.2: Applications processing and underwriting

Examples of good practice	Examples of poor practice
• A firm's underwriting process can identify applications that may, based on a thorough assessment of risk flags relevant to the firm, present a higher risk of mortgage fraud. • Underwriters can contact all parties to the application process (customers, brokers, valuers etc.) to clarify aspects of the application. • The firm verifies that deposit monies for a mortgage transaction are from a legitimate source. • New or inexperienced underwriters receive training about mortgage fraud risks, potential risk indicators, and the firm's approach to tackling the issue.	• A firm's underwriters have a poor understanding of potential fraud indicators, whether through inexperience or poor training. • Underwriters' demanding work targets undermine efforts to contain mortgage fraud. • A firm does not allocate responsibility for countering mortgage fraud clearly within the management hierarchy. • A firm relying on manual underwriting has no checklists to ensure the application process is complete. • A firm requires underwriters to justify all declined applications to brokers.

Box 11.3: Mortgage fraud prevention, investigations and recoveries

Examples of good practice	Examples of poor practice
• A firm routinely assesses fraud risks during the development of new mortgage products, with particular focus on fraud when it enters new areas of the mortgage market (such as sub-prime or buy-to-let).	• A firm's anti-fraud efforts are uncoordinated and under-resourced. • Fraud investigators lack relevant experience or knowledge of mortgage fraud issues, and have received insufficient training.

Box 11.3: Mortgage fraud prevention, investigations and recoveries

Examples of good practice	Examples of poor practice
• A firm reviews existing mortgage books to identify fraud indicators. • Applications that are declined for fraudulent reasons result in a review of pipeline and back book cases where associated fraudulent parties are identified. • A firm has planned how counter-fraud resources could be increased in response to future growth in lending volumes, including consideration of the implications for training, recruitment and information technology. • A firm documents the criteria for initiating a fraud investigation. • Seeking consent from the Serious Organised Crime Agency (SOCA) to accept mortgage payments wherever fraud is identified.	• A firm's internal escalation procedures are unclear and leave staff confused about when and how to report their concerns about mortgage fraud.

Box 11.4: Managing relationships with conveyancers, brokers and valuers

Examples of good practice	Examples of poor practice
• A firm has identified third parties they will not deal with, drawing on a range of internal and external information. • A third party reinstated to a panel after termination is subject to fresh due diligence checks. • A firm checks that conveyances register charges over property with the Land Registry in good time and chases this up. • Where a conveyancer is changed during the processing of an application, lenders contact both the original and new conveyancer to ensure the change is for a legitimate reason. • A firm checks whether third parties maintain professional indemnity cover. • A firm has a risk-sensitive process for subjecting property valuations to independent checks.	• A firm's scrutiny of third parties is a one-off exercise; membership of a panel is not subject to ongoing review. • A firm's panels are too large to be manageable. No work is undertaken to identify dormant third parties. • A firm solely relies on the Financial Services Register to check mortgage brokers, while scrutiny of conveyancers only involves a check of public material from the Law Society or Solicitors Regulation Authority. • A firm that uses divisional sales managers to overesee brokers has not considered how to manage conflics of interest that may arise.

Box 11.4: Managing relationships with conveyancers, brokers and valuers

Examples of good practice

- A firm can detect brokers 'gaming' their systems, for example by submitting applications designed to discover the firm's lending thresholds, or submitting multiple similar applications known to be within the firm's lending policy.
- A firm verifies that funds are dispersed in line with instructions held, particularly where changes to the Certificate of Title occur just before completion.

Box 11.5: Compliance and internal audit

Examples of good practice

- A firm has subjected anti-fraud measures to 'end-to-end' scrutiny, to assess whether defences are coordinated, rather than solely reviewing adherence to specific procedures in isolation.
- There is a degree of specialist anti-fraud expertise within the compliance and internal audit functions.

Examples of poor practice

- A firm's management of third party relationships is subject to only cursory oversight by compliance and internal audit.
- Compliance and internal audit staff demonstrate a weak understanding of mortgage fraud risks, because of inexperience or deficient training.

Box 11.6: Staff recruitment and vetting

Examples of good practice

- A firm requires staff to disclose conflicts of interest stemming from their relationships with third parties such as brokers or conveyancers.
- A firm has considered what enhanced vetting methods should be applied to different roles (e.g. credit checks, criminal record checks, CIFAS staff fraud database, etc).
- A firm adopts a risk-sensitive approach to managing adverse information about an employee or new candidate.
- A firm seeks to identify when a deterioration in employees' financial circumstances may indicate increased vulnerability to becoming involved in fraud.

Examples of poor practice

- A firm uses recruitment agencies without understanding the checks they perform on candidates, and without checking whether they continue to meet agreed recruitment standards.
- Staff vetting is a one-off exercise.
- Enhanced vetting techniques are applied only to staff in Approved Persons positions.
- A firm's vetting of temporary or contract staff is less thorough than checks on permanent staff in similar roles.

Box 11.7: Remuneration structures

Examples of good practice

- A firm has considered whether remuneration structures could incentivise behaviour that may increase the risk of mortgage fraud.
- A firm's bonuses related to mortgage sales will take account of subsequent fraud losses, whether through an element of deferral or by 'clawback' arrangements.

Examples of poor practice

- The variable element of a firm's remuneration of mortgage salespeople is solely driven by the volume of sales they achieve, with no adjustment for sales quality or other qualitative factors related to compliance.
- The variable element of salespeople's remuneration is excessive.
- Staff members' objectives fail to reflect any consideration of mortgage fraud prevention.

Box 11.8: Staff training and awareness

Examples of good practice

- A firm's financial crime training delivers clear messages about mortgage fraud across the organisation, with tailored training for staff closest to the issues.
- A firm verifies that staff understand training materials, perhaps with a test.
- Training is updated to reflect new mortgage fraud trends and types.
- Mortgage fraud 'champions' offer guidance or mentoring to staff.

Examples of poor practice

- A firm fails to provide adequate training on mortgage fraud, particularly to staff in higher-risk business areas.
- A firm relies on staff reading up on the topic of mortgage fraud on their own initiative, without providing formal training support.
- A firm fails to ensure mortgage lending policies and procedures are readily accessible to staff.
- A firm fails to define mortgage fraud in training documents or policies and procedures.
- Training fails to ensure all staff are aware of their responsibilities to report suspicions, and the channels they should use.

12.
Banks' management of high money-laundering risk situations (2011)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **banks** we supervise under the Money Laundering Regulations 2007. Boxes 12.1 – 12.4 also apply to other **firms** we supervise under the Money Laundering Regulations **that have customers who present a high money-laundering risk**. It may be of interest to other firms we supervise under the Money Laundering Regulations 2007.

Content: This chapter contains sections on:

12.1 In June 2011 the *FSA* published the findings of its thematic review of how banks operating in the UK were managing money-laundering risk in higher-risk situations. The *FSA* focused in particular on correspondent banking relationships, wire transfer payments and high-risk customers including politically exposed persons (PEPs). The *FSA* conducted 35 visits to 27 banking groups in the UK that had significant international activity exposing them to the AML risks on which the *FSA* were focusing.

12.2 The *FSA's* review found no major weaknesses in banks' compliance with the legislation relating to wire transfers. On correspondent banking, there was a wide variance in standards with some banks carrying out good quality AML work, while others, particularly among the smaller banks in the *FSA's* sample, carried out either inadequate due diligence or none at all.

12.3 However, the *FSA's* main conclusion was that around three-quarters of banks in its sample, including the majority of major banks, were not always managing high-risk customers and PEP relationships

effectively and had to do more to ensure they were not used for money laundering purposes. The *FSA* identified serious weaknesses in banks' systems and controls, as well as indications that some banks were willing to enter into very high-risk business relationships without adequate controls when there were potentially large profits to be made. This meant that the *FSA* found it likely that some banks were handling the proceeds of corruption or other financial crime.

12.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

The FSA's findings

12.5 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf

Consolidated examples of good and poor practice

12.6 In addition to the examples of good and poor practice below, Section 6 of the report also included case studies illustrating relationships into which banks had entered which caused the *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

Box 12.1: High-risk customers and PEPs – AML policies and procedures

Examples of good practice	Examples of poor practice
• Senior management take money laundering risk seriously and understand what the Money Laundering Regulations are trying to achieve. • Keeping AML policies and procedures up to date to ensure compliance with evolving legal and regulatory obligations • A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff. • Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis. • Ensuring adequate due diligence has been carried out on all customers, even if they have been referred by somebody who is powerful or influential or a senior manager. • Providing good quality training to relevant staff on the risks posed by higher risk customers including PEPs and correspondent banks.	• A lack of commitment to AML risk management among senior management and key AML staff. • Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice. • Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs. • Failing to carry out enhanced due diligence on customers with political connections who, although they do not meet the legal definition of a PEP, still represent a high risk of money laundering. • Giving waivers from AML policies without good reason. • Considering the reputational risk rather than the AML risk presented by customers. • Using group policies which do not comply fully with UK AML legislation and regulatory requirements. • Using consultants to draw up policies which are then not implemented. • Failing to allocate adequate resources to AML.

Box 12.1: High risk customers and PEPs – AML policies and procedures

Examples of good practice	Examples of poor practice
• Ensuring RMs[9] and other relevant staff understand how to manage high money laundering risk customers by training them on practical examples of risk and how to mitigate it. • Keeping training material comprehensive and up-to-date, and repeating training where necessary to ensure relevant staff are aware of changes to policy and emerging risks.	• Failing to provide training to relevant staff on how to comply with AML policies and procedures for managing high-risk customers. • Failing to ensure policies and procedures are easily accessible to staff.

Box 12.2: High-risk customers and PEPs – risk assessment

Examples of good practice	Examples of poor practice
• Using robust risk assessment systems and controls appropriate to the nature, scale and complexities of the bank's business. • Considering the money-laundering risk presented by customers, taking into account a variety of factors including, but not limited to, company structures; political connections; country risk; the customer's reputation; source of wealth/funds; expected account activity; sector risk; and involvement in public contracts. • Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite. • Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff. • Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice. • Appropriately weighted scores for risk factors which feed in to the overall customer risk assessment. • A clear audit trail to show why customers are rated as high, medium or low risk.	• Allocating higher risk countries with low risk scores to avoid having to conduct EDD. • MLROs who are too stretched or under resourced to carry out their function appropriately. • Failing to risk assess customers until shortly before an FCA visit. • Allowing RMs to override customer risk scores without sufficient evidence to support their decision. • Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.

9 Relationship Managers.

Box 12.3: High-risk customers and PEPs – customer take-on

Examples of good practice

- Ensuring files contain a customer overview covering risk assessment, documentation, verification, expected account activity, profile of customer or business relationship and ultimate beneficial owner.
- The MLRO (and their team) have adequate oversight of all high-risk relationships.
- Clear processes for escalating the approval of high risk and all PEP customer relationships to senior management or committees which consider AML risk and give appropriate challenge to RMs and the business.
- Using, where available, local knowledge and open-source Internet checks to supplement commercially available databases when researching potential high-risk customers including PEPs.
- Having clear risk-based policies and procedures setting out the EDD required for higher risk and PEP customers, particularly in relation to source of wealth.
- Effective challenge of RMs and business units by banks' AML and compliance teams, and senior management.
- Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated.
- Clearly establishing and documenting PEP and other high-risk customers' source of wealth.
- Where money laundering risk is very high, supplementing CDD with independent intelligence reports and fully exploring and reviewing any credible allegations of criminal conduct by the customer.
- Understanding and documenting complex or opaque ownership and corporate structures and the reasons for them.
- Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.
- Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships.

Examples of poor practice

- Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations definition of a PEP (eg wider family) which might mean that certain customers still need to be treated as high risk and subject to enhanced due diligence.
- Poor quality, incomplete or inconsistent CDD.
- Relying on group introductions where overseas standards are not UK-equivalent or where CDD is inaccessible due to legal constraints.
- Inadequate analysis and challenge of information found in documents gathered for CDD purposes.
- Lacking evidence of formal sign-off and approval by senior management of high-risk and PEP customers and failure to document appropriately why the customer was within AML risk appetite.
- Failing to record adequately face-to-face meetings that form part of CDD.
- Failing to carry out EDD for high-risk/PEP customers.
- Failing to conduct adequate CDD before customer relationships are approved.
- Over-reliance on undocumented 'staff knowledge' during the CDD process.
- Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason.
- Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports.
- Failing to carry out CDD on customers because they were referred by senior managers.
- Failing to ensure CDD for high-risk and PEP customers is kept up to date in line with current standards.
- Allowing 'cultural difficulties' to get in the way of proper questioning to establish required CDD records.

Box 12.3: High-risk customers and PEPs – customer take-on

Examples of good practice	Examples of poor practice
• Recognising and mitigating the risk arising from RMs becoming too close to customers and conflicts of interest arising from RMs' remuneration structures.	• Holding information about customers of their UK operations in foreign countries with banking secrecy laws if, as a result the firm's ability to access or share CDD is restricted. • Allowing accounts to be used for purposes inconsistent with the expected activity on the account (e.g. personal accounts being used for business) without enquiry. • Insufficient information on source of wealth with little or no evidence to verify that the wealth is not linked to crime or corruption. • Failing to distinguish between source of funds and source of wealth. • Relying exclusively on commercially available PEP databases and failure to make use of available open-source information on a risk-based approach. • Failing to understand the reasons for complex and opaque offshore company structures. • Failing to ensure papers considered by approval committees present a balanced view of money laundering risk. • No formal procedure for escalating prospective customers to committees and senior management on a risk-based approach. • Failing to take account of credible allegations of criminal activity from reputable sources. • Concluding that adverse allegations against customers can be disregarded simply because they hold an investment visa. • Accepting regulatory and/or reputational risk where there is a high risk of money laundering.

Box 12.4: High risk customers and PEPs – enhanced monitoring of high-risk relationships

Examples of good practice

- Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds.
- Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP.
- Monitoring new clients more closely to confirm or amend the expected account activity.
- A risk-based framework for assessing the necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring.
- Proactively following up gaps in, and updating, CDD during the course of a relationship.
- Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives.
- Keeping good records and a clear audit trail of internal suspicion reports sent to the MLRO, whether or not they are finally disclosed to SOCA.
- A good knowledge among key AML staff of a bank's highest risk/PEP customers.
- More senior involvement in resolving alerts raised for transactions on higher risk or PEP customer accounts, including ensuring adequate explanation and, where necessary, corroboration of unusual transactions from RMs and/or customers.
- Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs.
- Assessing RMs' performance on ongoing monitoring and feeding this into their annual performance assessment and pay review.
- Lower transaction monitoring alert thresholds for higher-risk customers.

Examples of poor practice

- Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD.
- Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review.
- Failing to disclose suspicious transactions to SOCA.
- Failing to seek consent from SOCA on suspicious transactions before processing them.
- Unwarranted delay between identifying suspicious transactions and disclosure to SOCA.
- Treating annual reviews as a tick-box exercise and copying information from the previous review.
- Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment.
- Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs.
- Failing to update CDD based on actual transactional experience.
- Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP customers.
- Failing to apply sufficient challenge to explanations from RMs and customers about unusual transactions.
- RMs failing to provide timely responses to alerts raised on transaction monitoring systems.

Box 12.5: Correspondent banking – risk assessment of respondent banks

Examples of good practice	Examples of poor practice
• Regular assessments of correspondent banking risks taking into account various money laundering risk factors such as the country (and its AML regime); ownership/management structure (including the possible impact/influence that ultimate beneficial owners with political connections may have); products/operations; transaction volumes; market segments; the quality of the respondent's AML systems and controls and any adverse information known about the respondent. • More robust monitoring of respondents identified as presenting a higher risk. • Risk scores that drive the frequency of relationship reviews. • Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.	• Failing to consider the money-laundering risks of correspondent relationships. • Inadequate or no documented policies and procedures setting out how to deal with respondents. • Applying a 'one size fits all' approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries. • Failing to prioritise higher risk customers and transactions for review. • Failing to take into account high-risk business types such as money service businesses and offshore banks.

Box 12.6: Correspondent banking – customer take-on

Examples of good practice	Examples of poor practice
• Assigning clear responsibility for the CDD process and the gathering of relevant documentation. • EDD for respondents that present greater risks or where there is less publicly available information about the respondent. • Gathering enough information to understand client details; ownership and management; products and offerings; transaction volumes and values; client market segments; client reputation; as well as the AML control environment. • Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose. • Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.	• Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction. • Collecting CDD information but failing to assess the risks. • Over-relying on the Wolfsberg Group AML questionnaire. • Failing to follow up on outstanding information that has been requested during the CDD process. • Failing to follow up on issues identified during the CDD process. • Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done. • Collecting AML policies etc but making no effort to assess them.

Box 12.6: Correspondent banking – customer take-on

Examples of good practice

- Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country.
- Identifying risk in particular business areas (e.g. informal vallue transfer such as 'hawala', tax evasion, corruption) through discussion with overseas regulatiors.
- Visiting, or otherwise liaising with, respondent banks to discuss AML issues and gather CDD information.
- Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs.
- Understanding respondents' processes for monitoring account activity and reporting suspicious activity.
- Requesting details of how respondents manage their own correspondent banking relationships.
- Senior management/senior committee sign-off for new correspondent banking relationships and reviews of existing ones.

Examples of poor practice

- Having no information on file for expected activity volumes and values.
- Failing to consider adverse information about the respondent or individuals connected with it.
- No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.

Box 12.7: Correspondent banking – ongoing monitoring of respondent accounts

Examples of good practice

- Review periods driven by the risk rating of a particular relationship; with high-risk relationships reviewed more frequently.
- Obtaining an updated picture of the purpose of the account and expected activity.
- Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists.
- Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high-risk relationships.
- Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.

Examples of poor practice

- Copying periodic review forms year after year without challenge from senior management.
- Failing to take account of any changes to key staff at respondent banks.
- Carrying out annual reviews of respondent relationships but failing to consider money-laundering risk adequately.
- Failing to assess new information gathered during ongoing monitoring of a relationship.
- Failing to consider money laundering alerts generated since the last review.
- Relying on parent banks to carry out monitoring of respondents without understanding what monitoring has been done or what the monitoring found.

Box 12.7: Correspondent banking – ongoing monitoring of respondent accounts	
Examples of good practice	Examples of poor practice
• Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.	• Failing to take action when respondents do not provide satisfactory answers to reasonable questions regarding activity on their account. • Focusing too much on reputational or business issues when deciding whether to exit relationships with respondents which give rise to high money-laundering risk.

Box 12.8: Wire transfers – paying banks	
Examples of good practice	Examples of poor practice
• Banks' core banking systems ensure that all static data (name, address, account number) held on the ordering customer are automatically inserted in the correct lines of the outgoing MT103 payment instruction and any matching MT202COV.	• Paying banks take insufficient steps to ensure that all outgoing MT103s contain sufficient beneficiary information to mitigate the risk of customer funds being incorrectly blocked, delayed or rejected.

Box 12.9: Wire transfers – intermediary banks	
Examples of good practice	Examples of poor practice
• Where practical, intermediary and beneficiary banks delay processing payments until they receive complete and meaningful information on the ordering customer. • Intermediary and beneficiary banks have systems that generate an automatic investigation every time a MT103 appears to contain inadequate payer information. • Following processing, risk-based sampling for inward payments identifies inadequate payer information. • Search for phrases in payment messages such as 'one of our clients' or 'our valued customer' in all the main languages which may indicate a bank or customer trying to conceal their identity.	• Banks have no procedures in place to detect incoming payments containing meaningless or inadequate payer information, which could allow payments in breach of sanctions to slip through unnoticed.

Box 12.10: Wire transfers – beneficiary banks

Examples of good practice	Examples of poor practice
• Establishing a specialist team to undertake risk-based sampling of incoming customer payments, with subsequent detailed analysis to identify banks initiating cross-border payments containing inadequate or meaningless payer information. • Actively engaging in dialogue with peers about the difficult issue of taking appropriate action against persistently offending banks.	• Insufficient processes to identify payments with incomplete or meaningless payer information.

Box 12.11: Wire transfers – implementation of SWIFT MT202COV

Examples of good practice	Examples of poor practice
• Reviewing all correspondent banks' use of the MT202 and MT202COV. • Introducing the MT202COV as an additional element of the CDD review process including whether the local regulator expects proper use of the new message type. • Always sending an MT103 and matching MT202COV wherever the sending bank has a correspondent relationship and is not in a position to 'self clear' (eg for euro payments within a scheme of which the bank is a member). • Searching relevant fields in MT202 messages for the word 'cover' to detect when the MT202COV is not being used as it should be.	• Continuing to use the MT202 for all bank-to-bank payments, even if the payment is cover for an underlying customer transaction.

13.
Anti-bribery and corruption systems and controls in investment banks (2012)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply to:

- **investment banks** and firms carrying on investment banking or similar activities in the UK;
- **all other firms** who are subject to our financial crime rules in SYSC 3.2.6R or 6.1.1R; and
- **electronic money institutions** and payment institutions within our supervisory scope.

Box **13.4** and Box **13.5** only apply to **firms or institutions who use third parties to win business**.

Content: This chapter contains sections on:

13.1 In March 2012, the *FSA* published the findings of its review of investment banks' anti-bribery and corruption systems and controls. The *FSA* visited 15 investment banks and firms carrying on investment banking or similar activities in the UK to assess how they were managing bribery and corruption risk. Although this report focused on investment banking, its findings are relevant to other sectors.

13.2 The *FSA* found that although some investment banks had completed a great deal of work to implement effective anti-bribery and corruption controls in the months preceding its visit, the majority of them had more work to do and some firms' systems and controls fell short of its regulatory requirements. Weaknesses related in particular to: many firms' limited understanding of the applicable legal and regulatory regimes, incomplete or inadequate bribery and corruption risk assessments; lack of senior management oversight; and failure to monitor the effective implementation of, and compliance with, anti-bribery and corruption policies and procedures.

13.3 The contents of this report are reflected in Chapter 6 (Bribery and corruption) of Part 1 of this Guide.

13.4 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/pubs/other/anti-bribery-investment-banks.pdf

Box 13.1: Governance and management information (MI)

Examples of good practice	Examples of poor practice
• Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate terms of reference and senior management membership, reporting ultimately to the Board. • Regular and substantive MI to the Board and other relevant senior management forums, including: an overview of the bribery and corruption risks faced by the business; systems and controls to mitigate those risks; information about the effectiveness of those systems and controls; and legal and regulatory developments. • Where relevant, MI includes information about third parties, including (but not limited to) new third-party accounts, their risk classification, higher risk third-party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties. • Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis. • Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.	• Failing to establish an effective governance framework to address bribery and corruption risk. • Failing to allocate responsibility for anti-bribery and corruption to a single senior manager or an appropriately formed committee. • Little or no MI sent to the Board about bribery and corruption issues, including legislative or regulatory developments, emerging risks and higher risk third-party relationships or payments.

Box 13.2: Assessing bribery and corruption risk

Examples of good practice

- Responsibility for carrying out a risk assessment and keeping it up to date is clearly apportioned to an individual or a group of individuals with sufficient levels of expertise and seniority.
- The firm takes adequate steps to identify the bribery and corruption risk. Where internal knowledge and understanding of corruption risk is limited, the firm supplements this with external expertise.
- Risk assessment is a continuous process based on qualitative and relevant information available from internal and external sources.
- Firms consider the potential conflicts of interest which might lead business units to downplay the level of bribery and corruption risk to which they are exposed.
- The bribery and corruption risk assessment informs the development of monitoring programmes; policies and procedures; training; and operational processes.
- The risk assessment demonstrates an awareness and understanding of firms' legal and regulatory obligations.
- The firm assesses where risks are greater and concentrates its resources accordingly.
- The firm considers financial crime risk when designing new products and services.

Examples of poor practice

- The risk assessment is a one-off exercise.
- Efforts to understand the risk assessment are piecemeal and lack coordination.
- Risk assessments are incomplete and too generic.
- Firms do not satisfy themselves that staff involved in risk assessment are sufficiently aware of, or sensitised to, bribery and corruption issues.

Box 13.3: Policies and procedures

Examples of good practice

- The firm clearly sets out the behaviour expected of those acting on its behalf.
- Firms have conducted a gap analysis of existing bribery and corruption procedures against applicable legislation, regulations and guidance and made necessary enhancements.
- The firm has a defined process in place for dealing with breaches of policy.
- The team responsible for ensuring the firm's compliance with its anti-bribery and corruption obligations engages with the business units about the development and implementation of anti-bribery and corruption systems and controls.
- anti-bribery and corruption policies and procedures will vary depending on a firm's exposure to bribery and corruption risk. But in most cases, firms should have policies and procedures which cover expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms; and disciplinary sanctions for breaches. These policies need not be in a single 'ABC policy' document and may be contained in separate policies.
- There should be an effective mechanism for reporting issues to the team or committee responsible for ensuring compliance with the firm's anti-bribery and corruption obligations.

Examples of poor practice

- The firm has no method in place to monitor and assess staff compliance with anti-bribery and corruption policies and procedures.
- Staff responsible for the implementation and monitoring of anti-bribery and corruption policies and procedures have inadequate expertise on bribery and corruption.

Box 13.4: Third-party relationships and due diligence

Examples of good practice	Examples of poor practice
• Where third parties are used to generate business, these relationships are subject to thorough due diligence and management oversight. • Third-party relationships are reviewed regularly and in sufficient detail to confirm that they are still necessary and appropriate to continue. • There are higher, or extra, levels of due diligence and approval for high-risk third-party relationships. • There is appropriate scrutiny of, and approval for, relationships with third parties that introduce business to the firm. • The firm's compliance function has oversight of all third-party relationships and monitors this list to identify risk indicators, eg a third party's political or public service connections. • Evidence that a risk-based approach has been adopted to identify higher risk relationships in order to apply enhanced due diligence. • Enhanced due diligence procedures include a review of the third party's own anti-bribery and corruption controls. • Consideration, where appropriate, of compliance involvement in interviewing consultants and the provision of anti-bribery and corruption training to consultants. • Inclusion of anti-bribery and corruption-specific clauses and appropriate protections in contracts with third parties.	• A firm using intermediaries fails to satisfy itself that those businesses have adequate controls to detect and prevent staff using bribery or corruption to generate business. • The firm fails to establish and record an adequate commercial rationale for using the services of third parties. • The firm is unable to produce a list of approved third parties, associated due diligence and details of payments made to them. • There is no checking of compliance's operational role in approving new third-party relationships and accounts. • A firm assumes that long-standing third-party relationships present no bribery or corruption risk. • A firm relies exclusively on informal means, such as staff's personal knowledge, to assess the bribery and corruption risk associated with third parties. • No prescribed take-on process for new third-party relationships. • A firm does not keep full records of due diligence on third parties and cannot evidence that it has considered the bribery and corruption risk associated with a third-party relationship. • The firm cannot provide evidence of appropriate checks to identify whether introducers and consultants are PEPs. • Failure to demonstrate that due diligence information in another language has been understood by the firm.

Box 13.5: Payment controls

Examples of good practice	Examples of poor practice
• Ensuring adequate due diligence on and approval of third-party relationships before payments are made to the third party. • Risk-based approval procedures for payments and a clear understanding of the reason for all payments. • Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account. • Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments. • A healthily sceptical approach to approving third-party payments. • Adequate due diligence on new suppliers being added to the Accounts Payable system. • Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced. • Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable hospitality. • Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved. • The facility to produce accurate MI to assist effective payment monitoring.	• Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval. • Failing to produce regular third-party payment schedules for review. • Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality. • No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.

Box 13.6: Gifts and hospitality (G&H)

Examples of good practice	Examples of poor practice
• Policies and procedures clearly define the approval process and the limits applicable to G&H. • Processes for filtering G&H by employee, client and type of hospitality for analysis. • Processes to identify unusual or unauthorised G&H and deviations from approval limits for G&H. • Staff are trained on G&H policies to an extent appropriate to their role, in terms of both content and frequency, and regularly reminded to disclose G&H in line with policy. • Cash or cash-equivalent gifts are prohibited. • Political and charitable donations are approved at an appropriate level, with input from the appropriate control function, and subject to appropriate due diligence.	• Senior management do not set a good example to staff on G&H policies. • Acceptable limits and the approval process are not defined. • The G&H policy is not kept up to date. • G&H and levels of staff compliance with related policies are not monitored. • No steps are taken to minimise the risk of gifts going unrecorded. • Failure to record a clear rationale for approving gifts that fall outside set thresholds. • Failure to check whether charities being donated to are linked to **relevant political or administrative decision-makers**.

Box 13.7: Staff recruitment and vetting

Examples of good practice	Examples of poor practice
• Vetting staff on a risk-based approach, taking into account financial crime risk. • Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially available intelligence databases – for staff in roles with higher bribery and corruption risk. • Conducting periodic checks to ensure that agencies are complying with agreed vetting standards.	• Failing to carry out ongoing checks to identify changes that could affect an individual's integrity and suitability. • No risk-based processes for identifying staff who are PEPs or otherwise connected to **relevant political or administrative decision-makers**. • Where employment agencies are used to recruit staff, failing to demonstrate a clear understanding of the checks these agencies carry out on prospective staff. • Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

Box 13.8: Training and awareness

Examples of good practice	Examples of poor practice
• Providing good quality, standard training on anti-bribery and corruption for all staff. • Ensuring training covers relevant and practical examples. • Keeping training material and staff knowledge up to date. • Awareness-raising initiatives, such as special campaigns and events to support routine training, are organised.	• Failing to provide training on ABC that is targeted at staff with greater exposure to bribery and corruption risks. • Failing to monitor and measure the quality and effectiveness of training.

Box 13.9: Remuneration structures

Examples of good practice	Examples of poor practice
• Remuneration takes account of good compliance behaviour, not simply the amount of business generated. • Identifying higher-risk functions from a bribery and corruption perspective and reviewing remuneration structures to ensure they do not encourage unacceptable risk-taking.	• Failing to reflect poor staff compliance with anti-bribery and corruption policy and procedures in staff appraisals and remuneration.

Box 13.10: Incident reporting and management

Examples of good practice	Examples of poor practice
• Clear procedures for whistleblowing and the reporting of suspicions, which are communicated to staff. • Details about whistleblowing hotlines are visible and accessible to staff. • Where whistleblowing hotlines are not provided, firms should consider measures to allow staff to raise concerns in confidence or, where possible, anonymously, with adequate levels of protection and communicate this clearly to staff. • Firms use information gathered from whistleblowing and internal complaints to assess the effectiveness of their anti-bribery and corruption policies and procedures.	• Failing to maintain proper records of incidents and complaints.

14.
Banks' defences against investment fraud (2012)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **deposit-taking institutions** with retail customers.

Content: This chapter contains sections on:

14.1 The *FSA's* thematic review, Bank's defences against investment fraud, published in June 2012, set out the findings of its visits to seven retail banks and one building society to assess the systems and controls in place to contain the risks posed by investment fraudsters.

14.2 UK consumers are targeted by share-sale frauds and other scams including land-banking frauds, unauthorised collective investment schemes and Ponzi schemes. Customers of UK deposit-takers may fall victim to these frauds, or be complicit in them.

14.3 The contents of this report are reflected in new Box 4.5 in Chapter 4 (Fraud) of Part 1 of this Guide.

The FSA's findings

14.4 You can read the findings of the *FSA's* thematic review here:

http://www.fsa.gov.uk/static/pubs/other/banks-defences-against-investment-fraud.pdf

Consolidated examples of good and poor practice

14.5 In addition to the examples of good and poor practice below, Section 6 of the report also included case studies illustrating relationships into which banks had entered which caused the *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

Box 14.1: Governance

Examples of good practice	Examples of poor practice
• A bank can demonstrate senior management ownership and understanding of fraud affecting customers, including investment fraud. • There is a clear organisational structure for addressing the risk to customers and the bank arising from fraud, including investment fraud. There is evidence of appropriate information moving across this governance structure that demonstrates its effectiveness in use. • A bank has recognised subject matter experts on investment fraud supporting or leading the investigation process. • A bank seeks to measure its performance in preventing detriment to customers. • When assessing the case for measures to prevent financial crime, a bank considers benefits to customers, as well as the financial impact on the bank.	• A bank lacks a clear structure for the governance of investment fraud or for escalating issues relating to investment fraud. Respective responsibilities are not clear. • A bank lacks a clear rationale for allocating resources to protecting customers from investment fraud. • A bank lacks documented policies and procedures relating to investment fraud. • There a lack of communication between a bank's AML and fraud teams on investment fraud.

Box 14.2: Risk assessment

Examples of good practice	Examples of poor practice
• A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could suffer losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are also informed by this assessment. • A bank performs 'horizon scanning' work to identify changes in the fraud types relevant to the bank and its customers.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud. • A bank's regulatory compliance, risk management and internal audit functions' assurance activities do not effectively challenge the risk assessment framework.

Box 14.3: Detecting perpetrators

Examples of good practice	Examples of poor practice
• A bank's procedures for opening commercial accounts include an assessment of the risk of the customer, based on the proposed business type, location and structure. • Account opening information is used to categorise a customer relationship according to its risk. The bank then applies different levels of transaction monitoring based on this assessment. • A bank screens new customers to prevent the take-on of possible investment fraud perpetrators.	• A bank only performs the customer risk assessment at account set up and does not updating this through the course of the relationship. • A bank does not use account set up information (such as anticipated turnover) in transaction monitoring. • A bank allocates excessive numbers of commercial accounts to a staff member to monitor, rendering the ongoing monitoring ineffective. • A bank allocates responsibility for the ongoing monitoring of the customer to customer-facing staff with many other conflicting responsibilities.

Box 14.4: Automated monitoring

Examples of good practice	Examples of poor practice
• A bank undertakes real-time payment screening against data about investment fraud from credible sources. • There is clear governance of real time payment screening. The quality of alerts (rather than simply the volume of false positives) is actively considered. • Investment fraud subject matter experts are involved in the setting of monitoring rules. • Automated monitoring programmes reflect insights from risk assessments or vulnerable customer initiatives. • A bank has monitoring rules designed to detect specific types of investment fraud e.g. boiler room fraud. • A bank reviews accounts after risk triggers are tripped (such as the raising of a SAR) in a timely fashion. • When alerts are raised, a bank checks against account-opening information to identify any inconsistencies with expectations.	• A bank fails to use information about known or suspected perpetrators of investment fraud in its financial crime prevention systems. • A bank does not consider investment fraud in the development of monitoring rules. • The design of rules cannot be amended to reflect the changing nature of the risk being monitored.

Box 14.5: Protecting victims

Examples of good practice	Examples of poor practice
• A bank contacts customers in the event they suspect a payment is being made to an investment fraudster. • A bank places material on investment fraud on its website. • A bank adopts alternative customer awareness approaches, such as mailing customers and branch awareness initiatives. • Work to detect and prevent investment fraud is integrated with a bank's vulnerable customers initiative.	• Communication with customers on fraud just covers types of fraud for which the bank may be financially liable, rather than fraud the customer might be exposed to. • A bank has no material on investment fraud on its website. • Failing to contact customers they suspect are making payments to investment fraudsters on grounds that this constitutes 'investment advice'.

Box 14.6: Management reporting and escalation of suspicions

Examples of good practice	Examples of poor practice
• A specific team focuses on investigating the perpetrators of investment fraud. • A bank's fraud statistics include figures for losses known or suspected to have been incurred by customers.	• There is little reporting to senior management on the extent of investment fraud (whether victims or perpetrators) in a bank's customer base. • A bank is unable to access information on how many of the bank's customers have become the victims of investment fraud.

Box 14.7: Staff awareness

Examples of good practice	Examples of poor practice
• Making good use of internal experience of investment fraud to provide rich and engaging training material. • A wide range of materials are available that cover investment fraud. • Awards are given on occasion to frontline staff when a noteworthy fraud is identified. • Training material is tailored to the experience of specific areas such as branch and relationship management teams.	• Training material only covers boiler rooms. • A bank's training material is out of date.

Box 14.8: Use of industry intelligence

Examples of good practice	Examples of poor practice
• A bank participates in cross-industry forums on fraud and boiler rooms and makes active use of intelligence gained from these initiatives in, for example, its transaction monitoring and screening efforts. • A bank takes measures to identify new fraud typologies. It joins up internal intelligence, external intelligence, its own risk assessment and measures to address this risk.	• A bank fails to act on actionable, credible intelligence shared at industry forums or received from other authoritative sources such as the FCA or City of London Police.

15.
Banks' control of financial crime risks in trade finance (2013)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **banks carrying out trade finance business**.

Content: This chapter contains sections on:

15.1 In July 2013, we published the findings of our review of banks' control of financial crime risks in trade finance. We visited 17 commercial banks to assess the systems and controls they had in place to contain the risks of money laundering, terrorist financing and sanctions breaches in trade finance operations. Our review only considered Documentary Letters of Credit (LCs) and Documentary Bills for Collection (BCs).

15.2 We found that banks generally had effective controls to ensure they were not dealing with sanctioned individuals or entities. But most banks had inadequate systems and controls over dual-use goods and their anti-money laundering policies and procedures were often weak.

15.3 The following examples of good and poor practice should be read in conjunction with Part 1 of this Guide. Part 1 provides more general guidance, including on AML and sanctions systems and controls, that can be relevant in the context of banks' trade finance business. Not all examples of good and poor practice will be relevant to all banks that carry out trade finance business and banks should consider them in a risk-based and proportionate way.

15.4 You can read the findings of the *FSA's* thematic review here:

http://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf

Consolidated examples of good and poor practice

Box 15.1: Governance and MI

Examples of good practice	Examples of poor practice
• Roles and responsibilities for managing financial crime risks in trade finance are clear and documented. • The bank ensures that staff have the opportunity to share knowledge and information about financial crime risk in trade finance, for example by holding regular teleconferences with key trade finance staff or by including trade finance financial crime risk as an agenda item in relevant forums.	• Failure to produce management information on financial crime risk in trade finance. • Internal audit fails to consider financial crime controls in trade finance. • The culture of a bank does not encourage the sharing of information relevant to managing financial crime risk in trade finance.

Box 15.2: Risk assessment

Examples of good practice	Examples of poor practice
• The bank assesses and documents both money laundering and sanctions risk in the bank's trade finance business. This assessment is tailored to the bank's role in trade transactions and can form part of the bank's wider financial-crime risk assessment.	• Failure to update risk assessments and keep them under regular review to take account of emerging risks in trade finance. • Only focusing on credit and reputational risk in trade finance. • Not taking account of a customer's use of the bank's trade finance products and services in a financial crime risk assessment.

Box 15.3: Policies and procedures

Examples of good practice	Examples of poor practice
• Staff are required to consider financial crime risks specific to trade finance transactions and identify the customers and transactions that present the highest risk at various stages of a transaction. • Staff identify key parties to a transaction and screen them against sanctions lists. Key parties include the instructing party, but may include other parties on a risk-sensitive basis. • The bank provides guidance on recognising red flags in trade finance transactions.	• Staff are not required to consider trade specific money laundering risks (eg FATF/ Wolfsberg red flags). • Procedures do not take account of money laundering risks and are focused on credit and operational risks. • No clear escalation procedures for high-risk transactions. • Procedures fail to take account of the parties involved in a transaction, the countries where they are based and the nature of the good inolved.

Box 15.4: Due diligence

Examples of good practice	Examples of poor practice
• Banks' written procedures are clear about what due diligence checks are necessary on the instructing parties. They take account of the bank's role in a transaction, and when it is appropriate to apply due diligence checks to others, including non-client beneficiaries (or recipients) of an LC or BC.	• Trade processing teams do not make adequate use of the significant knowledge of customers' activity possessed by relationship managers or trade sales teams when considering the financial crime risk in particular transactions. • Lack of appropriate dialogue between CDD teams and trade processing teams whenever potential financial crime issues arise from the processing of a trade finance transaction.

Box 15.5: Training and awareness

Examples of good practice	Examples of poor practice
• Tailored training is given that raises staff awareness and understanding of trade-specific money laundering, sanctions and terrorist financing risks. • Relevant industry publications are used to raise awareness of emerging risks. • Processing staff are trained to look for suspicious variances in the pricing of comparable or analogous transactions.	• Only providing generic training that does not take account of trade-specific AML risks (eg FATF/Wolfsberg red flags). • Failure to roll out trade specific financial crime training to all relevant staff engaged in trade finance activity, wherever located. • Reliance on 'experienced' trade processing staff who have received no specific training on financial crime risk.

Box 15.6: AML procedures

Examples of good practice	Examples of poor practice
• A formal consideration of money laundering risk is written into the operating procedures governing LCs and BCs. • The money laundering risk in each transaction is considered and evidence of the assessment made is kept. • Detailed guidance is available for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags. • Staff processing transactions have a good knowledge of a customer's expected activity; and a sound understanding of trade based money laundering risks. • Processing teams are encouraged to escalate suspicions for investigation as soon as possible.	• Failure to assess transactions for money laundering risk. • Reliance on customer due diligence procedures alone to mitigate the risk of money laundering in transactions. • Reliance on training alone to ensure that staff escalate suspicious transactions, when there are no other procedures or controls in place. • Disregarding money laundering risk when transactions present little or no credit risk. • Money laundering risk is disregarded when transactions involve another group entity (especially if the group entity is in a high risk jurisdiction). • A focus on sanctions risk at the expense of money laundering risk.

Box 15.6: AML procedures

Examples of good practice	Examples of poor practice
• Those responsible for reviewing escalated transactions have an extensive knowledge of trade-based money laundering risk. • Underlying trade documentation relevant to the financial instrument is obtained and reviewed on a risk-sensitive basis. • Third party data sources are used on a risk-sensitive basis to verify the information given in the LC or BC. • Using professional judgement to consider whether the pricing of goods makes commercial sense, in particular in relation to traded commodities for which reliable and up-to-date pricing information can be obtained. • Regular, periodic quality assurance work is conducted by suitably qualified staff who assess the judgments made in relation to money laundering risk and potentially suspicious transactions. • Trade processing staff keep up to date with emerging trade-based money laundering risks. • Where red flags are used by banks as part of operational procedures, they are regularly updated and easily accessible to staff. • Expertise in trade-based money laundering is also held in a department outside of the trade finance business (e.g. Compliance) so that independent decisions can be made in relation to further investigation of escalations and possible SAR reporting.	• Failure to document adequately how money laundering risk has been considered or the steps taken to determine that a transaction is legitimate. • Trade-based money laundering checklists are used as 'tick lists' rather than as a starting point to think about the wider risks. • Failure to investigate potentially suspicious transactions due to time constraints or commercial pressures. • Failure to ensure that relevant staff understand money laundering risk and are aware of relevant industry guidance or red flags. • Failure to distinguish money laundering risk from sanctions risk. • Ambiguous escalation procedures for potentially suspicious transactions, or procedures that only allow for escalation to be made to sanctions teams. • Not taking account of other forms of potentially suspicious activity that may not be covered by the firm's guidance. • Failure to make use of information held in CDD files and RMs' knowledge to identify potentially suspicious transactions. • Trade processing teams are not given sufficient time to fully investigate potentially suspicious activity, particularly when there are commercial time pressures. • Trade processing staff are not encouraged to keep up to date with emerging trade based money laundering risks.

Box 15.7: Sanctions procedures

Examples of good practice	Examples of poor practice
• Screening information is contained within trade documents against applicable sanctions lists. • Hits are investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made. • Shipping container numbers are validated on a risk-sensitive basis. • Potential sanctions matches are screened for at several key stages of a transaction. • Previous sanction alerts are analysed to identify situations where true hits are most likely to occur and the bank focuses its sanctions resources accordingly. • New or amended information about a transaction is captured and screened.	• Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced to perform the role effectively. • Failure to screen trade documentation. • Failure to screen against all relevant international sanctions lists. • Failure to keep up to date with the latest information regarding name changes for sanctioned entities, especially as the information may not be reflected immediately on relevant sanctions list. • Failure to record the rationale for decisions to discount false positives. • Failure to undertake risk-sensitive screening of information held on agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin, as well as the main counterparties to a transaction. • Failure to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes.

Box 15.8: Dual-use goods

Examples of good practice	Examples of poor practice
• Ensuring staff are aware of dual-use goods issues, common types of goods that have a dual use, and are capable of identifying red flags that suggest that dual-use goods risk being supplied for illicit purposes. • Confirming with the exporter in higher risk situations whether a government licence is required for the transaction and seeking a copy of the licence where required.	• No clear dual-use goods policy. • Failure to undertake further research where goods descriptions are unclear or vague. • Third party data sources are not used where possible to undertake checks on dual-use goods.

16.
How small banks manage money laundering and sanctions risk – update (2014)

Who should read this chapter? This chapter is relevant, and its statements of good practice apply, to **banks** we supervise under the Money Laundering Regulations 2007. It may be of interest to **other firms** we supervise under the Money Laundering Regulations 2007.

Content: This chapter contains sections on:

16.1 In November 2014 we published the findings of our thematic review of how small banks manage AML and sanctions risk. We assessed the adequacy of the AML and sanctions systems and controls of 21 small banks. We also looked at the extent to which the banks had considered our regulatory AML guidance, enforcement cases and the findings from our 2011 review of 'banks' management of high money laundering risk situations'. To this end, our sample included five banks that had also been part of our sample in 2011.

16.2 A small number of banks in our sample had implemented effective AML and sanctions controls. But, despite our extensive work in this area over recent years, we found significant and widespread weaknesses in most of the sample banks' AML systems and controls and some banks' sanctions controls. We also found that AML resources were inadequate in one-third of all banks in our sample and that some overseas banks struggled to reconcile their group AML policies with UK AML standards and requirements.

16.3 The contents of this report are reflected in Chapters 1, 2 and 3 of Part 1 of this Guide.

16.4 You can read the findings of our thematic review here: http://www.fca.org.uk/news/tr14-16-how-small-banks-manage-money-laundering-and-sanctions-risk

Box 16.1: Management information (MI)

Useful MI provides senior management with the information they need to ensure that the firm effectively manages the money laundering and sanctions risks to which it is exposed. MI should be provided regularly, including as part of the MLRO report, and ad hoc, as risk dictates.

Examples of useful MI include:

- an overview of the money laundering and sanctions risks to which the bank is exposed, including information about emerging risks and any changes to the bank's risk assessment
- an overview of the systems and controls to mitigate those risks, including information about the effectiveness of these systems and controls and any changes to the bank's control environment
- legal and regulatory developments and the impact these have on the bank's approach
- relevant information about individual business relationships, for example:
  - the number and nature of new accounts opened, in particular where these are high risk
  - the number and nature of accounts closed, in particular where these have been closed for financial crime reasons
  - the number of dormant accounts and re-activated dormant accounts, and
  - the number of transaction monitoring alerts and suspicious activity reports, including where the processing of these has fallen outside of agreed service level agreements.

Box 16.2: Governance structures

Banks should have a governance structure that is appropriate to the size and nature of their business.

To be effective, a governance structure should enable the firm to:

- clearly allocate responsibilities for financial crime issues
- establish clear reporting lines and escalation paths
- identify and manage conflicts of interest, in particular where staff hold several functions cumulatively, and
- record and retain key decisions relating to the management of money laundering and sanctions risks, including, where appropriate, decisions resulting from informal conversations.

Box 16.3: Culture and tone from the top

An effective AML and sanctions control framework depends on senior management setting and enforcing a clear level of risk appetite, and embedding a culture of compliance where financial crime is not acceptable.

Examples of good practice include:

- senior management taking leadership on AML and sanctions issues, for example through everyday decision-making and staff communications
- clearly articulating and enforcing the bank's risk appetite – this includes rejecting individual business relationships where the bank is not satisfied that it can manage the risk effectively
- allocating sufficient resources to the bank's compliance function
- ensuring that the bank's culture enables it to comply with the UK's legal and regulatory AML framework, and
- considering whether incentives reward unacceptable risk-taking or compliance breaches and, if they do, removing them.

Box 16.4: Risk assessment

ML Reg 20
SYSC 6.3.1R

Banks must identify and assess the money laundering risk to which they are exposed. This will help them understand which parts of their business are most vulnerable to money laundering and which parts they should prioritise in their fight against financial crime. It will also help banks decide on the appropriate level of CDD and monitoring for individual business relationships.

A business-wide risk assessment:

- must be comprehensive, meaning that it should consider a wide range of factors, including the risk associated with the bank's customers, products, and services – it is not normally enough to consider just one factor
- should draw on a wide range of relevant information – it is not normally enough to consider just one source, and
- must be proportionate to the nature, scale and complexity of the bank's activities.

Banks should build on their business-wide risk assessment to determine the level of CDD they should apply to individual business relationships or occasional transactions. CDD will help banks refine their assessment of risk associated with individual business relationships or occasional transactions and will determine whether additional CDD measures should be applied and the extent of monitoring that is required to mitigate that risk. An individual assessment of risk associated with a business relationship or occasional transaction can inform, but is no substitute for, a business-wide risk assessment.

A customer risk assessment:

- should enable banks to take a holistic view of the risk associated with a business relationship or occasional transaction by considering all relevant risk factors, and
- should be recorded – where the risk is high, banks should include the reason why they are content to accept the risk associated with the business relationship or occasional transaction and details of any steps the bank will take to mitigate the risks, such as restrictions on the account or enhanced monitoring.

Box 16.5: Enhanced due diligence (EDD)

The central objective of EDD is to enable a bank to better understand the risks associated with a high-risk customer and make an informed decision about whether to on-board or continue the business relationship or carry out the occasional transaction. It also helps the bank to manage the increased risk by deepening its understanding of the customer, the beneficial owner, and the nature and purpose of the relationship.

ML Reg 7

The extent of EDD must be commensurate with the risk associated with the business relationship or occasional transaction but banks can decide, in most cases, which aspects of CDD they should enhance.

Senior management should be provided with all relevant information (eg, source of wealth, source of funds, potential risks, adverse information and red flags) before approving PEP relationships to ensure they understand the nature of, and the risks posed by, the relationship they are approving.

Examples of effective EDD measures we observed included:

- obtaining more information about the customer's or beneficial owner's business
- obtaining more robust verification of the beneficial owner's identity on the basis of information obtained from a reliable and independent source
- carrying out searches on a corporate customer's directors (or individuals exercising control) to understand whether their business or integrity affects the level of risk associated with the business relationship, for example because they also hold a public function
- using open source websites to gain a better understanding of the customer or beneficial owner, their reputation and their role in public life – where banks find information containing allegations of wrongdoing or court judgments, they should assess how this affects the level of risk associated with the business relationship
- establishing the source of wealth to be satisfied that this is legitimate – banks can establish the source of wealth through a combination of customer-provided information, open source information and documents such as evidence of title, copies of trust deeds and audited accounts (detailing dividends)
- establishing the source of funds used in the business relationship to be satisfied they do not constitute the proceeds of crime
- commissioning external third-party intelligence reports where it is not possible for the bank to easily obtain information through open source searches or there are doubts about the reliability of open source information, and
- where the bank considers whether to rely on another firm for EDD purposes, it ensures that the extent of EDD measures is commensurate with the risk it has identified and that it holds enough information about the customer to carry out meaningful enhanced ongoing monitoring of the business relationship – the bank must also be satisfied that the quality of EDD is sufficient to satisfy the UK's legal and regulatory requirements.

Box 16.6: Enhanced ongoing monitoring

In addition to guidance contained in Part 1 Box 3.8 of ***Financial crime: a guide for firms***:

- compliance has adequate oversight over the quality and effectiveness of periodic and event-driven reviews, and
- the firm does not place reliance only on identifying large transactions and makes use of other 'red flags'.

Transaction monitoring

Examples of red flags in transaction monitoring can include (this list is not exhaustive):

- third parties making repayments on behalf of the customer, particularly when this is unexpected
- repayments being made from multiple bank accounts held by the customer
- transactions that are inconsistent with the business activities of the customer
- the purpose of the customer account changing without adequate explanation or oversight
- transactions unexpectedly involving high-risk jurisdictions, sectors or individuals
- early repayment of loans or increased frequency/size of repayments
- accounts with low balances but a high volume of large debits and credits
- cumulative turnover significantly exceeding the customer's income/expected activity
- debits being made shortly after credits of the same value are received
- the customer making frequent transactions just below transaction monitoring alert thresholds
- debits to and credits from third parties where there is no obvious explanation for the transaction, and
- the customer providing insufficient or misleading information when asked about a transaction, or being otherwise evasive.

Customer reviews

ML Reg 8

Banks must keep the documents, data or information obtained as part of the CDD process up to date. This will help banks ascertain that the level of risk associated with the business relationship has not changed, or enable them to take appropriate steps where it has changed.

Examples of factors which banks may consider when conducting periodic reviews.

- Has the nature of the business relationship changed?
- Does the risk rating remain appropriate in the light of any changes to the business relationship since the last review?
- Does the business relationship remain within the firm's risk appetite?
- Does the actual account activity match the expected activity indicated at the start of the relationship? If it does not, what does this mean?

Examples of measures banks may take when reviewing business relationships:

- assessing the transactions flowing through the customer's accounts at a business relationship level rather than at an individual transaction level to identify any trends
- repeating screening for sanctions, PEPs and adverse media, and
- refreshing customer due diligence documentation, in particular where this is not in line with legal and regulatory standards.

Box 16.7: Sanctions

In addition to guidance contained in Part 1 Chapter 7 of *Financial crime: a guide for firms*, examples of good practice include:

- firms carrying out 'four-eye' checks on sanctions alerts before closing an alert or conducting quality assurance on sanctions alert closure on a sample basis
- firms regularly screening their customer database (including, where appropriate, associated persons, eg, directors) against sanctions lists using systems with fuzzy matching capabilities, and
- specified individuals having access to CDD information held on each of the bank's customers to enable adequate discounting of sanctions alerts.

17. Managing bribery and corruption risk in commercial insurance broking – update (2014)

Who should read this chapter? This chapter is relevant, and its statements of good practice apply, to

- **commercial insurance intermediaries and other firms** who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R, and
- **e-money institutions and payment institutions** within our supervisory scope.

Content: This chapter contains sections on:

17.1 In November 2014 we published a thematic review of how commercial insurance intermediaries manage bribery and corruption risk. We looked at ten intermediaries' anti-corruption systems and controls and the extent to which these intermediaries had considered our existing guidance, enforcement cases and the findings from thematic work, particularly our 2010 review of 'anti-bribery and corruption in wholesale insurance broking'. This sample also included five intermediaries that had been part of the sample in 2010.

17.2 While most intermediaries had begun to look at their ABC systems and controls, this was work in progress and more improvement was needed. We found that most intermediaries we saw were still not managing their bribery and corruption risk effectively. Business-wide bribery and corruption risk assessments were based on a range of risk factors that were too narrow and many intermediaries failed to take a holistic view of the bribery and corruption risk associated with individual relationships. Half of the due diligence files we reviewed were inadequate and senior management oversight was often weak.

17.3 The contents of this report are reflected in Chapters 1 and 2 of Part 1 of this Guide.

17.4 You can read the findings of our thematic review here: http://www.fca.org.uk/news/tr14-17-managing-bribery-and-corruption-risk-in-commercial-insurance-broking

Box 17.1: Governance

This section complements guidance in Part 1, Boxes 2.1 and 6.1 and Part 2, Box 9.1

- As part of their ABC governance structures, intermediaries may consider appointing an ABC officer with technical expertise and professional credibility within the intermediary.
- Intermediaries should ensure that responsibility for oversight and management of third-party introducers and other intermediaries is clearly allocated.

Box 17.2: Management information (MI)

This section complements guidance in Part 1, Boxes 2.1A and 6.1 and Part 2, Box 9.1

Examples of ABC MI which intermediaries may consider providing include:

- details of any business rejected in the relevant period because of bribery and corruption concerns, including the perception that the risk of bribery and corruption associated with the business might be increased, and
- details, using a risk-based approach, of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected and cases of non-compliance with the intermediary's policies where relevant.

Intermediaries may consider providing ABC MI about third-party introducers and other intermediaries.

Examples of such MI include:

- a breakdown of third-party introducers and other intermediaries, in chains that are involved in business generation, with details of the business sectors and countries they work in
- the amount of business each third-party introducer or other intermediary generates
- how much the immediate third-party introducer or other intermediary with whom the intermediary has a direct relationship is paid and on what basis (fees, commission, etc), and
- details of the third-party introducer's role, including the services they provide and the basis of the commission or other remuneration they receive.

Box 17.3: Risk assessment

This section complements guidance in Part 1, Boxes 2.3 and 6.2 and Part 2, Boxes 9.2 and 9.3

Business-wide risk assessments

Intermediaries should identify and assess the bribery and corruption risk across all aspects of their business.

Examples of factors which intermediaries should consider when assessing risk across their business.

- Risks associated with the jurisdictions the intermediary does business in, the sectors they do business with and how they generate business.
- Risks associated with insurance distribution chains, in particular where these are long. This includes taking steps to understand the risk associated with parties that are not immediate relationships, where these can be identified. Parties that are not immediate relationships may include, in addition to the insured and the insurer, entities such as introducers, sub-brokers, co-brokers, producing brokers, consultants, coverholders and agents.
- Risks arising from non-trading elements of the business, including staff recruitment and remuneration, corporate hospitality and charitable donations.

Risk assessments and due diligence for individual relationships

The risk-rating process for individual third-party introducer and client relationships, for example the producing broker, should build on the intermediary's business-wide risk assessment.

Examples of factors intermediaries may consider when assessing bribery and corruption risk associated with individual relationships include:

- the role that the party performs in the distribution chain
- the territory in which it is based or in which it does business
- how much and how the party is remunerated for this work
- the risk associated with the industry sector or class of business, and
- the governance and ownership of the third party, including any political or governmental connections.

Intermediaries should decide on the level of due diligence, and which party to apply due diligence to, based on their assessment of risk associated with the relationship. This may include other parties in the insurance chain and not just their immediate contact. Where it is not possible or feasible to conduct due diligence on other parties, intermediaries should consider alternative approaches, such as adjustments to the level of monitoring to identify unusual or suspicious payments.

Examples of the type of information which intermediaries may obtain as part of the due diligence process include:

- other intermediaries' terms of business and identification documentation, including information about their anti-corruption controls
- checks, as risk dictates, on company directors, controllers and ultimate beneficial owners, considering any individuals or companies linked to the client, PEP screening and status, links to a PEP or national government, sanctions screening, adverse media screening and action taken in relation to any screening hits, and
- for third-party introducers, details of the business rationale.

Box 17.4: Ongoing monitoring and reviews

This section complements guidance in Part 1, Boxes 2.4, 6.3 and 6.4 and Part 2, Box 9.3

Examples of ongoing monitoring and review for ABC purposes include:

- payment monitoring, including a review of payments to identify unusual or suspicious payments
- refreshing due diligence documentation
- ensuring that the business rationale remains valid – this may include a review of third-party introducers' activities
- re-scoring risk where necessary, including based on the outcome of internal or external reviews or audits
- updating PEP screening, sanctions screening and adverse media screening, and
- taking a risk-based approach to ongoing monitoring measures applied to directors, controllers, ultimate beneficial owners and shareholders relevant to third-party relationships, which is consistent with the risk rating applied at the outset of a relationship.

Box 17.5: Payment controls – insurance broking accounts

This section complements guidance in Part 1, Boxes 6.3 and 6.4 and Part 2, Boxes 9.4 and 9.9

- Intermediaries should set meaningful thresholds for gifts and hospitality that reflect business practice and help identify potentially corrupt actions.
- When determining whether a payment is appropriate, staff responsible for approving payments should consider whether the payment is in line with the approved scope of the third-party relationship.

Box 17.6: Payment controls – accounts payable

This section complements guidance in Part 1, Boxes 6.3 and 6.4 and Part 2, Box 9.4

- Intermediaries should consider whether an absence of recorded gifts, entertainment, expenses and donations may be due to reporting thresholds being too high and/or staff being unaware of the requirement to report.

Box 17.7: Training and awareness

This section complements guidance in Part 1, Boxes 2.5 and 6.3 and Part 2, Boxes 9.6 and 9.9

Examples of initiatives to supplement ABC training and awareness include:

- creating a one-page aide-mémoire for staff, listing key points on preventing financial crime and the whistleblowing process, to which staff could easily refer, and
- appointing a compliance expert within each business area who provides ABC advice to staff.

Financial Conduct Authority

25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
Website: www.fca.org.uk