

## Chapter 5

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

5.3 Consolidated examples of good and  
poor practice

5.3.1

Firms’ implementation of a risk-based approach to AML

Examples of good practice	Examples of poor practice
<ul style="list-style-type: none"><li>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.</li><li>One building society undertook a comprehensive policy</li></ul>	<ul style="list-style-type: none"><li>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 (Money Laundering Reporting Officer. See <a href="#">FCG Annex 1</a> for common terms) 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.</li><li>Some small firms had produced inadequate annual</li></ul>

review following the publication of the 2006 JMLSG (Joint Money Laundering Steering Group. See [FCG Annex 1](#) for common terms) 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 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

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 (Suspicious Activity Report. See [FCG Annex 1](#) for common terms) 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.

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.

- 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.

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.