Money Laundering bulletin
The monthly briefing service for anti-laundering specialists

Independent AML audit – essential element or nice to have?

In comparing transatlantic notes, one of us, ***Ross Delston****, an American and the other,* ***Martin Owen****, a British anti-money laundering expert, we have both been struck by the contrast between the focus on independent audit in the United States and other jurisdictions on the one hand and the European lack of emphasis on the other. We decided to explore further.*

By 'independent audit' we mean review, by persons who are not part of the anti-money laundering / counter financing of terrorism (AML/CFT) compliance team, of the firm's AML/CFT policies and procedures, for their appropriateness, compliance and effectiveness. (As with other core features of an AML program, independent audit is relevant not just to banks but to other kinds of financial institution; and now indeed to the designated non-financial businesses and professions (such as solicitors, accountants, estate agents) required to have AML systems and controls.) We are not referring to the financial audit done by the firm's external chartered or certified public accountants to meet securities or company law requirements. The independent audit for AML may be done by external accountants, but also by independent consultants, solicitors or the firm's own internal audit department.

Independent AML audit seems to be an AML nice-to-have in the UK and the EU, but a big deal in the rest of the world.

Global standards

It's not clear quite why this should be. If we look at the Financial Action Task Force (FATF) Recommendations, Recommendation 15 states that financial institutions' anti-money laundering programs should include "an audit function to test the system". And the FATF AML/CFT Methodology for Assessing Compliance with the FATF 40+9 Recommendations says that "financial institutions should be required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with [these] procedures, policies and controls." [1]

In the United States, independent audit is one of the four pillars of an AML program (along with: a system of compliance controls, a designated AML compliance officer and training). [2] Implementation of the independent audit requirement is also one of the first elements that US financial regulators look at when conducting an on-site examination of a firm's compliance with AML rules and the manual that US bank examiners use (and, by default, other financial regulators as well) sets forth in excruciating detail the many aspects of the firm's AML program that must be tested. [3]

In Australia, the latest version (February 2007) of the proposed rules under their new AML regime stipulates that the firm's risk-based approach assessment and its risk awareness and employee due diligence programs should be subject to "regular independent review": to assess their effectiveness, whether they comply with the Rules, whether they have been effectively implemented and whether the entity complies with the programs. The results of the review, and any report, must be provided to senior management. [4]

Singapore's new AML regime requires banks to "maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements." [5]

The Hong Kong AML Guidelines say that "internal audit also has an important part to play in independently evaluating on a periodic basis an institution's policies and procedures on money laundering." This is reflected in the self-assessment regime used in Hong Kong. [6]

Under the Canadian regime, banks are required to establish a system of independent procedures testing to be conducted by the internal audit department, compliance department, or by an outside party. Deficiencies are to be reported to senior management and the board of directors with a summary of steps taken or to be taken to address any deficiencies. [7]

EU and UK standards

This all makes the EU generally and the UK specifically seem surprisingly reticent on the topic.

Independent audit does not figure explicitly in the EU Third Directive, which simply requires firms to have appropriate policies and procedures for "internal control". [8] We can perhaps charitably assume that "appropriate" must include provision for independent review, but the terms of the Article do not suggest that review, let alone independent review, are AML priorities.

The position in the UK is interesting.

The principle of an annual review is contained in the FSA rules, but it is the MLRO, not an independent party, who has to report at least annually on the operation and effectiveness of the AML systems and controls. And it is the firm itself that has to carry out a regular assessment of the systems and controls to ensure their continued compliance with the rules. [9]

Understandably, given this FSA perspective, the Joint Money Laundering Steering Group (JMLSG) Guidance contains no recommendations for independent review. It gives guidance only on the MLRO's annual report, with merely a passing reference to including a "report on the outcome of any relevant quality assurance or internal audit reviews of the firm's AML/CFT procedure." [10] Perhaps recognizing the brevity of even this guidance, the JMLSG published an aide mémoire in December 2006 that gives much more detailed guidance. [11] It is not clear why this should be outside rather than inside the main Guidance.

Practice

Of course practice does not always correspond to legal or regulatory obligation. But our personal impressions, rightly or wrongly, are that there is far more periodic independent audit in the US than in the UK. In the US, firms routinely use independent audit not just because it is required by law, regulation and examination manual, but also to give the firm advance warning of possible problem areas before a regulatory examination and indeed to provide a framework for the examination. They know that one of the first documents which a US examiner will ask the firm to supply will be any independent audit reports, and that the examiners will home in on deficiencies revealed, recommendations and follow-up actions committed to or taken (and if the recommendations were not implemented, why not?). Due to the regulatory requirement for an independent review, the US AML consulting industry has developed a routine practice of providing this service, tailored in scope and cost to institutions across the spectrums of risk and size.

In the UK, major firms at least commission a periodic external review. So, AML audit is also a substantial part of the UK AML consulting business. But, to a much greater extent than in the US, audits are done after-the-event, following regulatory problems, or on an occasional basis. This is not surprising – if the MLRO is required to invest the internal resource in his or her own review, what is the incentive to spend scarce resources on an additional internal or external audit that is not required by law, regulation or JMLSG Guidance?

We have no reason to believe that the integrity and the competence of UK MLROs and US AML compliance officers are very different. There is, however, a fundamental difference of approach in the two countries. In the UK, the principle is – trust the MLRO. In the US, the attitude is – if there are compliance problems, then the BSA [*Bank Secrecy Act*] compliance officer is unlikely to be the sole source for identifying and addressing them.

With US and elsewhere experience in mind, let's look more closely at the fundamentals of independent AML audits.

Who?

The independent audit may be done by internal or external auditors. Whoever does it must be qualified to do so and independent of the AML compliance group within the firm. External sources may be more expensive, but are particularly useful when internal resources with the necessary expertise and independence are not available.

Independence means not just being outside the specialist AML team. It means not being in the same reporting line. It also means not having had any responsibility for drafting, or for implementing the firm's AML programme. In other words, this will disqualify an external consulting firm that has been involved in devising the AML policies and procedures or a third party administrator or service provider who is charged with implementing those policies and procedures (eg, by acting as an external compliance officer or MLRO).

The expertise must be demonstrable. That normally means that any auditor, internal, external or consultant, must have had specialized AML training.

How often?

The greater the AML risk of the firm, and of the rate of change of the firm's business, the greater should be the frequency of audit. An annual audit is a good general rule. Given the constant and rapid change not

just in business but in AML requirements, risks and threats, the interval between audits should normally extend beyond 18 months only if the firm's business and the environment in which it operates are pretty static, which will not typically be the case.

What objective?

The objective of an independent audit is to form a view of the overall integrity and effectiveness of the AML programme, including policies, procedures, and processes. Put simply, does it work?

What scope?

In line with best practices for audits, the audit should be risk-based. The scope of the audit, and the frequency with which individual aspects of the AML programme are audited, should be a function of AML risk. Higher risk areas will need to be reviewed in every audit; lower risk areas can be reviewed on some form of rotational basis. The FATF Recommendations require a presumption that higher risk areas include at least international correspondent banking, non-face-to-face business (eg, on-line banking, lending or securities brokerage), and any operation that involves high levels of politically exposed persons (PEPs).

In this context, risk includes both intrinsic AML risk (eg, high risk customers) and compliance risk (eg, adequacy and implementation of the customer identification programme). Compliance risk should encompass learning any lessons from recent regulatory enforcement actions or pronouncements.

Any audit must also include the results of previous audits. A key element of the whole audit process is effective follow-up. Identification in a subsequent audit of failure to address recommendations and findings of previous audits should be a red flag to the board or audit committee – and will be in any regulatory inspection. (In this context, a fresh auditor will wish to satisfy himself/herself that the prior year's independent audit was indeed done by an independent and qualified auditor.)

What methods?

As with audit generally, the audit will involve: obtaining a good understanding of the firm's business and organisation, reviewing relevant core documents, transaction testing of the live application of policies and procedures, and interviewing a cross-section of players (and not just the AML team). The audit process must have sufficient depth and breadth to support the findings and to make the report worthwhile.

Who to whom?

The findings of the independent audit report, highlighting recommendations and deficiencies, should be reported to the CEO and senior management. They should also be sent to the board of directors or to the audit committee thereof, accompanied by the comments and recommendations of the AML compliance officer. This is not only best practice, but also a way of educating the board or audit committee about AML procedures, risks and problems that the firm faces.

The CEO, or other very senior executive, should take responsibility for agreeing to a follow-up action plan. The CEO, or some other senior officer to whom the task is delegated, should take ownership of this and ensure that it is implemented.

What topics?

Within the framework of the AML programme itself, the key topics to be addressed in an independent audit will be:

Core documentation

Are all the required core AML documents in place, duly approved, up-to-date and available to those who need them? A good-looking but out-of-date risk assessment is no good. Policy documents not approved by the board or top management lack authority. Updated procedures not disseminated to the front-line staff have no current value.

Risk assessment

Is the risk assessment comprehensive, does it use a robust methodology, and does it ring true? Does it cover all business lines, all target customers, all geographical relationships, including new ones introduced over the previous period? Does it reflect information and analysis, or just assertion? Does it reflect what the auditor knows of the company? Heaven forbid, is it unwritten? Although many firms seem to see risk as a matter of intuition, the regulators don't, and if they arrive only to find that a firm doesn't have a written risk assessment, the firm runs the risk that the regulators will do one for them!

Is the risk assessment a living document? Is there evidence that AML policies and procedures – and their implementation – do indeed reflect what the risk assessment identifies as the higher risk areas? Is the risk assessment applied in the handling of new

customers, new products, new channels, and new geographical ventures?

Policies

Do the policies and procedures explicitly reflect the risk assessment? Together, do they make a coherent whole? Or are the policies and procedures something someone took off the shelf, without any thought as to their applicability to the firm?

Are the key policies followed through into the firm's procedures and applied in practice? The policy document will cover matters like risk appetite for new customers, products or delivery channels, escalation expectations, watch lists to be used, training standards – are these reflected in the detailed procedures? Are the policies applied in practice?

Procedures

Are the stipulated procedures implemented in practice? Remember – this is a risk-based audit. So the focus should be on those procedures, and the contexts in which they are applied, that relate to the higher risk areas. Within this framework, the audit will need to cover all the main elements of the AML programme, including:

- **Customer identification:** Are the basic new customer (and sometimes new product) identification and verification procedures, and the arrangements for updating recorded data, applied effectively?
- **Enhanced customer due diligence (EDD):** Are the requirements for obtaining, verifying and maintaining additional information for higher risk customers or products applied effectively?
- **Name checking:** Are names and other data in incoming and outgoing wires and in other transactional activity checked against the Bank of England or other terrorist or the US OFAC watch lists used by the company? Are potential matches effectively followed up?
- **Enhanced monitoring of higher risk areas:** Do the line functions, and the AML systems, give additional scrutiny to higher risk customers, locations and products?
- **Transaction monitoring systems and methodologies:** Does the company have automated and manual systems that can cope with transactional volumes? Does any automated system use appropriate filters and detection scenarios? Does it support, and operate in a way that is consistent with, the firm's risk assessment?
- **Suspicious activity reporting:** Is there any indication of a systematic failure to identify transactions that need considering as potentially reportable? Or of any reluctance to make SARs in circumstances that appear to justify them? Is there adequate staff awareness across the whole business of their personal, as well as the firm's, obligations? Are confidentiality requirements strictly adhered to?
- **Cash or currency transaction reporting (if applicable):** Are reportable transactions identified and reports made within the applicable timescales?
- **Management information systems:** Are the board and senior management given sufficient information about AML activity, events and issues to enable them effectively to oversee the AML regime? Are management reports accurate?
- **Record-keeping:** Are accurate, legible records (eg, of customer identification or of SARs made) kept for the requisite period and readily accessible if needed?
- **Decision-making and governance:** Are escalation requirements and expectations met? Are decision-makers well-informed about the firm's risks profile and its compliance obligations? Do the board and senior management apply effective, well-informed oversight of the AML programme?
- **Training:** Is new staff given timely, adequate training? Are existing staff given adequate updates and refreshers? What about training of the board and senior management, easy to overlook, but at the very least, essential, and in some jurisdictions, like the US, required? Do specialist AML staff have sufficient opportunities to deepen and broaden their AML expertise and understanding of the business context? Is training comprehensive? Are materials accurate? Is attendance tracked? Is knowledge tested?
- **Resources:** Are the amount, and the expertise, of dedicated AML resources commensurate with the risk assessment and business volumes?

What deliverable?

The auditor should provide a signed, dated, written report that says who did the audit and when, describes the scope of the audit, and provides the results of the reviews, the weaknesses identified, and prioritized recommendations for further action. An audit report that is a terse paragraph or two that simply states all is OK will be a red flag to regulators. And the independent auditor's work papers should be kept, since, in the US, at least, examiners may ask for them.

Some Independent Audit Do's and Don'ts

1 Do time the audit to fit into the cycle of regular (eg, annual) board and top management reviews of AML risks and compliance and to anticipate any expected regulatory inspection. Scheduling it just before the regulators arrive for an on-site examination or inspection will raise red flags (yet, surprisingly, is done all the time!)
2 Do make sure that the independent auditor really is independent of the AML function in the firm – trying to fudge this one is a bad idea.
3 Do make sure that the independent auditor has adequate expertise – otherwise the audit may give false comfort or reach unjustified conclusions, or worse, the regulators will not take it seriously.
4 Do make sure that all stakeholders - the firm's board of directors, the audit committee, senior officers and relevant employees - understand that their full cooperation with the independent audit is a necessity.
5 Don't cut corners in cost or scope - the independent audit is a window into the compliance culture of the firm and therefore alerts the regulator to just how seriously (or not) the firm is taking AML compliance.
6 Don't fail to implement the recommendations of the independent audit or to record (hopefully good and justifiable) reasons why not. File and forget is not an option here.
7 Don't allow the audit plan to miss high risk products, operations and locations.
8 Do see independent audit in a positive light. A rigorous audit may seem like an ordeal. But a good auditor can often give you the benefit of his or her broad experience, and it is better to learn from an audit than from a regulatory inspection or an enforcement finding.

Worth greater focus?

You will gather that, whilst one of us writes 'program' and the other 'programme', we both agree that independent audit should be just as specific and explicit a part of AML program(me)s in the EU and the UK as in the rest of the world.

Notes

1 Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations. Recommendation 15. February 2007 edition, page 27.
2 USA PATRIOT Act, Sec. 352.
3 FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (2006), pp. 36 – 37.
4 Australian Transaction Reports and Analysis Centre. Draft Consolidated AML/CTF Rules for Discussion. 14 February 2007. 8.6
5 Monetary Authority of Singapore Notice 626 of 29 December 2006. 12.10
6 Hong Kong Monetary Authority Supplement of June 2004 to the Guideline on Prevention of Money Laundering, chapter 16.4. Dear Chief Executive letter of 30 June 2005 Self-Assessment of Compliance with Anti-Money Laundering (AML) Requirements sections 8.9-8.11
7 Office of the Superintendent of Financial Institutions. Guideline B-8. Deterring and Detecting Money Laundering and Terrorist Financing. II (c) (vi). November 2004
8 Article 34.1
9 Financial Services Authority Handbook. Senior Management Arrangements, Systems and Controls (SYSC) 6.3.7(2)G and 6.3.3R
10 Prevention of money laundering/combating the financing of terrorism. Guidance for the UK Financial Sector. Part 1. January 2006. 3.29-37
11 MLRO Annual Report. 4 December 2006

Ross Delston *is founder of GlobalAML.com, ross@globalaml.com, and* ***Martin Owen*** *is Vice President, Product Design, Haydrian Corporation, martin@haydrian.com.*