

Edward signalled to George, who opened the office door and stepped out. Edward turned in the door-frame as though something had just occurred to him. “Oh, yes – I forgot to say. All the records will need to be scanned as well – Ravi will bring up a scanner for you this afternoon and demonstrate how to use it. You can go for JPEGs or TIFs if you prefer, but we’d recommend PDFs for the most part.” He left Giles

sitting at his desk, frowning and silently mouthing “Peedy eff?”

#### Notes

1. See previous issues of *MLB*, from April 2010.

*Susan Grossey* may be contacted on +44 (0)1223 563636, [susan@thinkingaboutcrime.com](mailto:susan@thinkingaboutcrime.com)

## Due diligence: Know Your Process

*Relentless legislative change and riskier market conditions have led to renewed focus on due diligence screening processes. Long gone are the days when the business lunch was the standard method for screening a potential client or third-party agent. An effective due diligence process has become ever more critical to demonstrating robust compliance and protecting corporate reputation. However, in some firms the approach taken to due diligence has grown unchecked as business silos react in isolation to changing legislative and market demands. Mark Dunn of LexisNexis says that it is now time to take stock and review due diligence programmes to ensure that the business is maximising return on investment through quality output.*

The approach a company takes to due diligence screening is often dictated by the regulatory environment in which it operates and its appetite for risk. Market regulation has never been more prevalent and the risks facing business still emerging from the economic downturn continue to increase. These issues combine into a series of internal and external risks that companies seek to mitigate.

Take regulatory compliance – undertaking due diligence has long been a standard part of any anti-money laundering (AML) process as firms first determine and then apply a risk-based approach (RBA) to meet the simplified and enhanced customer due diligence requirements contained in the Money Laundering Regulations 2007 and the related checks required on beneficial owners and politically exposed persons (PEPs). Similarly, Schedule 7 of the *Counter Terrorism Act 2008* (CTA) gives HM Treasury the power to direct firms to conduct enhanced due diligence (EDD) where there is believed to be a risk of money laundering, terrorist financing or weapons of mass destruction (WMD) proliferation funding.

In turn, Acts like the CTA and a renewed focus by the Financial Services Authority (FSA) on the UK sanctions regime has also driven an increase in

screening as companies check customers and increasingly third-party agents, and even employees, against HM Treasury, EU and other international sanctions lists in line with their risk-based approach. Screening sanctions lists in some cases is not enough and firms increasingly also conduct checks against law enforcement ‘most wanted’ and similar global lists to ensure the organisation has done as much as it can to mitigate risk.

#### The Bribery Act 2010

The impending *Bribery Act 2010*, which is expected to come into force in April 2011, also emphasises the importance of undertaking due diligence. Both the Ministry of Justice (MoJ) draft guidance on the ‘adequate procedures’ that companies need to put in place to prevent bribery together with Transparency International’s own ‘The 2010 UK Bribery Act Adequate Procedures’ guidance, which preceded the MoJ’s document, emphasise effective due diligence processes. Unlike the Money Laundering Regulations 2007, where the focus is on customer due diligence (CDD), the guidance proposed for the *Bribery Act 2010* focuses on the importance of conducting due diligence on the company’s supply chain, its third-party agents and intermediaries and any joint venture partners or similar relationships. There is also some consideration given to employee screening. However, like the Money Laundering Regulations, the *Bribery Act 2010* guidance stresses the importance of conducting checks to manage the potential risks of doing business where ‘foreign public officials’ (effectively PEPs) are involved in business transactions. Much of the best practice applied to AML due diligence is now being applied to anti-bribery & corruption (ABC).

#### The fraud driver

Alongside regulatory compliance, heightened market risks are also driving the approach that companies take to

their due diligence processes. For example, the KPMG Fraud Barometer [1] continues to report the highest levels of fraud seen in the UK since the survey began 22 years ago. A closer look at the statistics indicates high levels of fraud committed by company directors (at an average of UK£4 million per case) and although not as widespread, employee fraud is still significant (for an average of UK£1 million per case). The primary weapon that companies can use to combat fraud is due diligence - undertaking comprehensive checks before a business transaction or new hire and continuing to monitor the individual or entity after the event to ensure the business has done all it can to mitigate financial or reputational risks. Alongside fraud, employee screening, increasingly, is also being extended to guard against other more extreme threats to the organisation.

The above selected examples of due diligence practice indicate just some of the existing and emerging requirements and how the focus on 'know your customer' (KYC) is shifting to encompass 'know your employee' (KYE), 'know your supplier' (KYS) and even 'know your customer's customer' (KYCC) as regulations and market drivers demand increased screening and ongoing monitoring activity. How companies have responded to these new challenges varies considerably. In many cases, companies have taken the traditional route of simply bolting on more and more resources to meet the demands of different departments and divisions. For example, across the organisation different levels of due diligence and screening are being conducted by different teams, including AML, Corporate Security, Fraud, Human Resources, Business Development, Procurement, Credit Risk, Strategy and Audit. All these separate teams are faced with tasks that encompass anything from running simple identity verification checks, conducting in-depth company research, undertaking third-party investigations, locating original company documents, running batches of names through sanctions and watch lists, checking against PEP lists, tracking supplier credit and payment data, searching media archives for reputational risks, researching networks of contacts, running conflicts checks and engaging outsourced risk advisors for specialist assignments.

### **A need to consolidate**

The outcome is that as the demand to complete more due diligence tasks has increased, the multitude of different research services purchased to meet individual departments' and divisions' needs has inevitably led to an overlap and duplication of those systems and

resources deployed. For example, several departments within the business may be subscribing to different identity verification service providers or multiple providers of UK or other local market company information, all effectively providing similar content and functionality. In the event, the organisation, through its silos, is managing multiple contracts for duplicate resources that deliver much the same data and services.

The inevitable result of utilising so many different products and services for due diligence tasks is inconsistency, inefficiency and high costs as each siloed department follows its own specific approach to due diligence using the resources it has chosen to deploy, unaware of what other departments are doing and the similarities in the services they are using. This can lead to bottlenecks in processing checks and an impact on internal and external customer service levels, leading to business delays. It is also more difficult to demonstrate consistent and robust compliance, maintain audit trails and train new Compliance and other analysts undertaking the checks when so many different systems are deployed. Further, it is difficult for the different teams across the business to share meaningful intelligence if the results of due diligence and other investigations have been conducted on different products and services that cover similar content but with minor differences in the data accessed, the search functionality applied and the format in which the results are retrieved and presented to the user. Ultimately, the greatest impact is on cost as the company is effectively paying several times over for overlapping products & services and missing out on the benefits of potential discounts from company-wide contracts.

To alleviate this overlap and duplication, firms' Compliance departments need to undertake a top-down review of the different due diligence tasks conducted across the organisation and also carry out a thorough audit of the various due diligence research tools and associated data content accessed across the business. This review needs to be aligned to the firm's risk-based approach to ensure that the due diligence services selected provide both the information required to help the firm comply with its regulatory obligations and also fulfil any additional investigative research tasks identified by the audit. For example, if the firm has corporate clients: are those companies public or private, based in the UK or overseas and in developed or emerging markets? All these issues will dictate the type of due diligence products and services required.

### Don't forget the consultants

The review should also take into account the firm's use of any third-party risk advisory consultants, who may have been contracted for due diligence or employee-screening tasks. It is important to assess the use of third parties as there may be some due diligence or screening tasks that the firm itself could undertake in-house with existing headcount, thereby reducing the amount of basic due diligence activity currently outsourced and the significant attendant cost. Instead, risk advisors could be deployed only on the specialist investigations and other projects where their unique skillset adds value, rather than on fairly fundamental due diligence research.

Undertaking due diligence has long been a key

process for any company conducting business and as regulatory requirements and market risks increase, there has been a significant change in the way firms need to approach the matter and better understand with whom their company is dealing. The *Bribery Act 2010* represents the latest legislative challenge and now is the time to review the approach to due diligence and to better prepare for the changing requirements ahead.

### Notes

1. Available at <http://rd.kpmg.co.uk/>

**Mark Dunn**, Market Planning Manager, Risk & Compliance:  
+44 (0) 20 7400 2984, [risk@lexisnexis.co.uk](mailto:risk@lexisnexis.co.uk)

## Banking on the border – San Marino and Italy

*On the border between Italy and the Most Serene Republic of San Marino, Italian Finance Police are a common sight. Their vigil took a technological twist last year with the appearance of mobile 'plurisensor' cameras possessing infrared and thermal sensors with the capacity to cross-reference motor registry databases, and detect vehicles carrying large sums of cash or valuables. The movement of money remains a sticky issue for institutions on both sides of the Italian/Sammarinese border as Lee Adendoorf reports, from Lucca, Italy.*

A 2010 International Monetary Fund (IMF) country report described San Marino as a “‘deposit-taking bank’ model characterised by bank secrecy, low taxation levels, and free circulation of capital to attract foreign capital”. The report indicates a financial sector that accounts for 18% of Gross Domestic Product (GDP) and more than 10% of government income.

This model preserved Italy's tax haven for years, but has left San Marino vulnerable to money laundering. The Council of Europe in its 2007 MONEYVAL report insisted San Marino urgently strengthen its banking rules and controls in order to meet international obligations of banking transparency.

Three years later, on a policy and legislation level there has been significant progress, which led to San Marino's removal from the Organisation for Economic Cooperation and Development's (OECD) 'grey' list of countries that had yet to implement global tax standards in September last year.

Four principal laws passed between 2008–2009 now

govern anti-money laundering (AML) and counter terrorist financing (CTF) practices among institutions. Highlights include the establishment of a Financial Intelligence Agency (to which significant resources have been dedicated), which is the AML/CTF monitoring and investigative body inside the Central Bank of San Marino. It also mandates financial institutions to report withdrawals or account closures exceeding €15,000; the regulation of frozen assets; and the obligatory declaration of transportation of cash and similar assets of more than €10,000.

The legislation has been accompanied, in the last 12 months, by the signing of 34 Memoranda of Understanding (MOUs) with the Financial Intelligence Units of other countries. However, a notably absent signatory on the list published in the agency's 2009 Annual Report is San Marino's most important partner nation, Italy.

Relations with Italy have been strained over the issue of banking transparency, especially after Italy's most recent tax amnesty saw more than €5 billion repatriated from San Marino. Although a database that allows for identity checks of account applicants through the exchange of information between San Marino and Italian banks was set up in 2009, the Italian Finance Ministry issued a statement on 11 May this year to confirm that San Marino remains on Italy's black list of tax havens.

This is no surprise given the scandals that have rocked San Marino over the last 18 months. The largest was the