KPMG
cutting through complexity

RISK CONSULTING

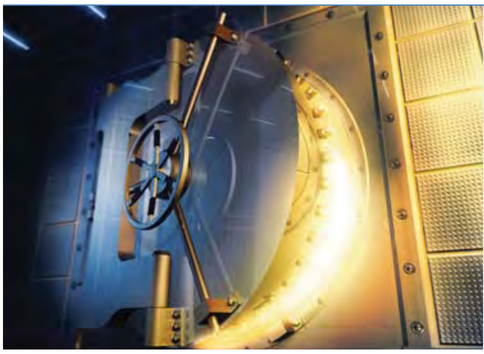
Global Anti-Money Laundering Survey
2011

How banks are facing up to the challenge

kpmg.com

According to an annual survey of the readers of *Operational Risk and Regulation* magazine on financial sector consultants conducted in 2008, 2009 and 2010.

Contents



Open
High
Low
Close
on Close (50)
on Close (100)
on Close (200)
838.63
856.45
836.23
845.12
NA
NA
NA

Jeremy Anderson
Global Head of Financial Services, KPMG

Brian Dilley
Global Head of Anti-Money Laundering, KPMG

Anti-Money Laundering compliance in a changing risk and regulatory world

We were both delighted and intrigued to embark once again on our Global Anti-Money Laundering (AML) Survey. Much has happened since our last survey in 2007, not least a major financial crisis that has shaken the global banking sector, regulators and governments alike to their cores.

It is no surprise, therefore, that while there is continued recognition of the importance of AML, many banking leaders have been preoccupied by issues such as capital and liquidity, credit issues, impairments, financial stability and stakeholders' demand for data, not to mention the very survival of their institutions.

Banks operating in multiple jurisdictions are making significant changes to their business models in response to the far-reaching global initiatives – such as those regulations imposed under Basel III and Dodd-Frank – that are changing the landscape they face.

In an environment of cost control, centered on preserving capital and prioritizing investment of precious resources on frontline business development, calls for a greater focus on AML can be a difficult sell.

AML is not receiving the board-level focus it used to, but its value should not be under-estimated

This shift in attention is evident from our latest research, which shows AML slipping down the boardroom agenda and no longer commanding the high profile it did in 2007.

Despite all the other pressures on boards, it is important that AML remains on the board agenda. Avoiding pitfalls in AML strategy and execution is key to preventing situations which will cause considerable management time to rectify and distract from other major strategic challenges.

While AML professionals may feel they are no longer at the center of their bank's risk management world, they still have a vital part to play. Their role in securing business benefits, covering off legal obligations and producing high quality data that can be used in multiple ways – including in the critical issue of managing credit risk – should not be forgotten.

With a clear duty to better understand the inter-dependencies and linkages within a bank – including between people, products, clients, systems and the business environment – senior executives need to reflect carefully as to how to use AML compliance more strategically as a tool to manage risk.

Strong AML processes also have the potential to enhance knowledge and coordination across departments – for instance which customers a bank may or may not wish to engage in business with, who they are, what they do and why they do it. This invaluable knowledge can be leveraged for the benefit of other teams, as well as for senior management's overall understanding of its customer base. Put simply, an organization that positively knows its clients can obtain a commercial advantage over rivals.

AML can inform a bank's risk appetite, critical to determining objectives and prioritizing spend

Articulating a bank's risk appetite is essential when interacting with regulators, whose general willingness to increase capital requirements – as well as the intensity of their overall scrutiny – has grown significantly in recent years.

Risk management since the crisis has been more focused on safety and soundness; there is evidence that the balance between prudential and conduct regulation is becoming more equal, and this sums up why the prominence of AML might appear diminished.

Clear understanding and communication of risk appetite can also help to optimize pan- and intra-departmental processes and controls. This is especially the case in larger banks operating in multiple jurisdictions, which are likely to be hit hardest by the G20-led regulations.

Management should feed what they learn from AML-related data, issues and challenges directly into the risk appetite debate, escalating to risk committees and audit committees where necessary.
Our firms' experience tells us that much of this data is duplicated across functions and locations, and that banks gain significant time and cost benefit from eliminating overlaps and becoming more efficient. The funds generated by reducing such process duplication and inefficiency will also have a direct impact on that bank's Tier 1 capital, a central driver of its ability to grow and leverage its balance sheet. Such theoretically straightforward analysis and review is too often not carried out, at a potential cost to a bank's capital position and its ability to optimally execute its business strategy.

AML can help to react to geopolitical events and cross-border regulatory developments

Events such as the 'Arab Spring' popular uprisings in the Middle East and North Africa, concern over the management of PEPs (as recently announced by the UK's Financial Services Authority and the topic of hearings and a report by the U.S. Congress' Permanent Sub-committee on Investigations), along with an evident ramping up of penalties and sanctions in many jurisdictions (especially in the U.S.), all mean that one does not need to look far for potent reminders of the importance of effective AML policies and controls.

The Arab Spring has considerable direct impact for AML compliance, one which could not have been anticipated. Taking the issue of PEPs to a new level is the question of how to deal with entire regimes against which sanctions are applied by the international community, or key players thereof. There is particularly heightened sensitivity surrounding regimes deemed to be corrupt or lacking in transparency.

Meanwhile, the rate of regulatory change continues at high speed, with the U.S. Foreign Account Tax Compliance Act (FATCA) due to take effect during 2013 and 2014, and EU Fourth Money Laundering Directive currently under development. The UK Bribery Act 2010 has already had a massive impact for AML teams around the world, especially in relation to PEP identification, and will continue to do so.

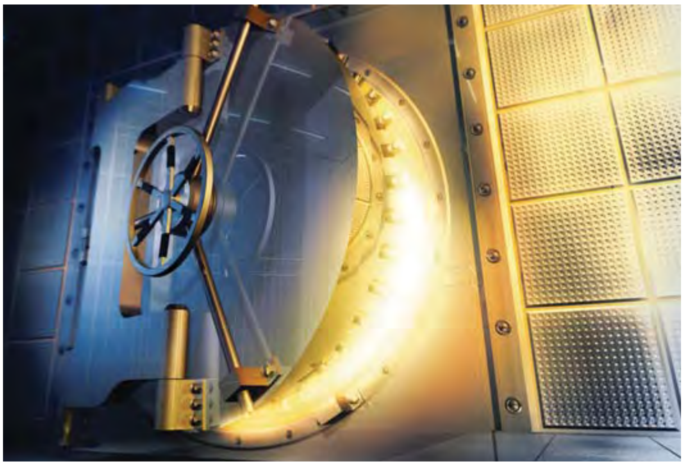
The extra-territorial reach of such legislation may raise the prominence of AML in regions such as Asia Pacific (ASPAC), where it appears to receive the least airtime among senior executives, and where investment in AML is expected to rise more slowly than elsewhere. In the case of FATCA (which has been supported by separate bilateral agreements reached between various countries), AML teams are likely to act as the 'first line of defense' against tax evasion, utilizing their due diligence activities to ensure that their institution meets the duties placed on it by national tax authorities to identify and report relevant account holders.

AML is more than just compliance

As well as making sure AML gets sufficient senior executive focus to ensure maximum effectiveness in a changing world, there is scope for it to make a more tangible contribution to the overall risk management effectiveness.

The other inevitable conclusion is that the next three years look set to be even busier than the last three for AML professionals, as they surely will be for other risk and regulatory professionals across the banking world. The key question to be answered is – will the pressures that are building in AML compliance combine to secure it the necessary attention and resources in the face of competing regulatory priorities?

In this multi-dimensional context, our survey provides insights into the many and varied challenges and trends facing AML teams. We would like to sincerely thank the 197 AML, compliance and other related specialists who participated in our survey for their contribution and perspectives.



Introduction and methodology

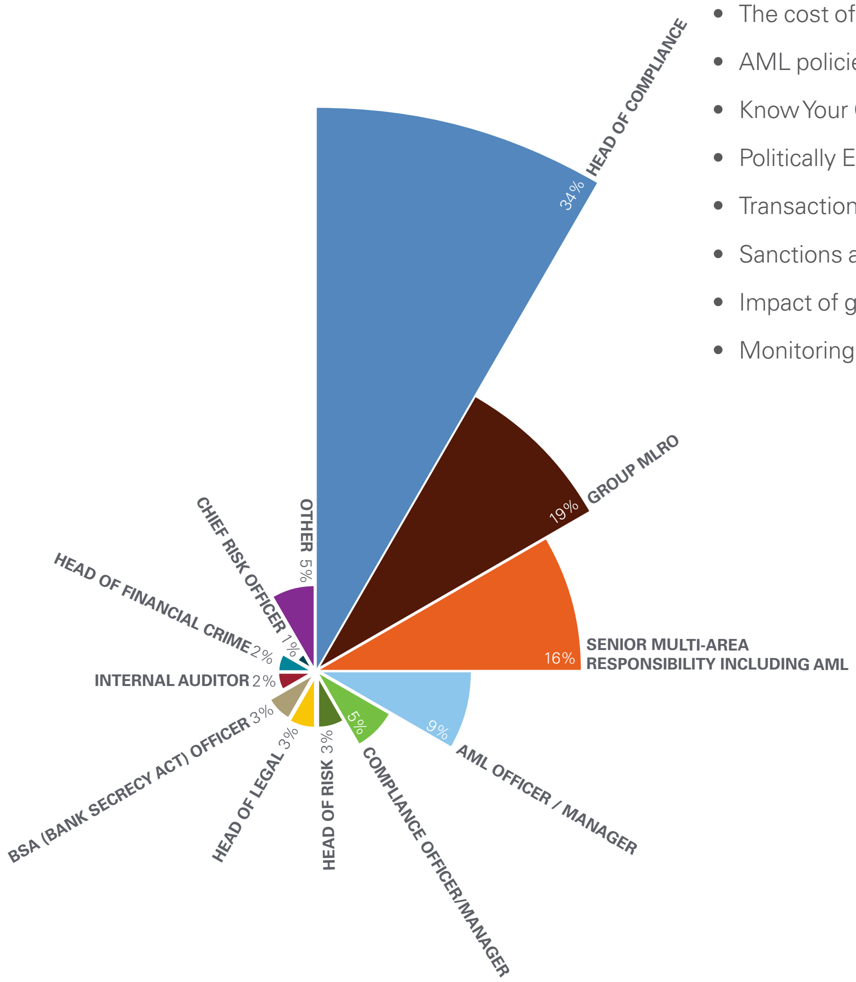
KPMG's Global AML Survey 2011 explores the range of strategic and implementation challenges that the international banking community faces in complying with evolving AML requirements. This is the third survey of its kind, following our previous research conducted in 2004 and 2007; the headlines from those reports are set out below.

Its overarching aims are to examine

- Perceptions of progress against money laundering and changes in the measures being used to combat it, including the reasons for progress (or lack of it) and for shifts in AML activity.
- Emerging trends and new threats, and perceptions of gaps in efforts to deal with these threats.
- Attitudes toward regulation and toward co-operation among the providers of financial and professional services and the governmental and international bodies working to control risks of financial crime including money laundering.

KPMG International commissioned RS Consulting, an independent research agency based in the United Kingdom, to conduct a telephone survey of banks across the major sectors (retail banking, corporate and business banking, private banking, investment banking and wholesale banking) during late 2010. These banks were drawn from the top 1,000 global banks according to the July 2010 edition of The Banker Magazine. The quality of respondents was high, with job titles ranging from Group Money Laundering Reporting Officer (MLRO) to Head of Compliance, Head of Legal and Head of Risk.

Respondents by job title



The survey covered the following topics

- The role of senior management in AML issues.
- The cost of AML compliance.
- AML policies and procedures.
- Know Your Customer (KYC) information.
- Politically Exposed Persons.
- Transaction monitoring.
- Sanctions and payments.
- Impact of global regulation and legislation.
- Monitoring of AML systems and controls.

KPMG Global AML Surveys – key headlines so far.

	2004	2007	2011
Priority for senior management	**AML was a relatively high priority within banks.** Sixty-one percent of respondent believed AML was a high profile issue for their senior management.	**Stronger senior management engagement in AML efforts.** Seventy-one percent of respondents stated that their board took an active interest in AML.	**Senior management interest has declined** but remains quite high, with 62 percent of respondents citing AML as a high profile issue.
Cost of compliance	**The cost of AML compliance increased sharply.** The average increase over the previous three years was 61 percent, with no respondents reporting a decrease in investment.	**AML costs grew beyond expectation.** Average costs grew 58 percent in the previous three years, compared to a prediction of 43 percent growth in 2004.	**Costs continue to rise**, at an average rate of 45 percent, against a prediction of 'over 40 percent' in 2007. **The extent of cost rises is underestimated by many.**
Taking a global approach	**Establishing a global policy was a major challenge.** Nearly two-thirds of respondents had a global AML policy in place; however half of these undertook implementation at a local level.	**Banks took a more global approach** to managing AML risk. 85 percent of internationally active banks had a global AML policy in place.	**There remains much variation in approach.** Two-thirds of banks have a global policy in place, however almost three quarters implement their procedures locally.
Testing and monitoring of controls	**Testing and monitoring of AML procedures needed to be independent and coordinated.** Senety-five percent of respondents had a formal program of independent testing.	**There was more monitoring of AML systems and controls.** Eighty-three percent of respondents formally tested and monitored the effectiveness of their systems and controls.	**The level of monitoring remains static**, with 84 percent formally testing their controls. Concern remains regarding the nearly one-fifth of respondents who do not do so.
Politically exposed persons	**PEPs were not a key area of focus,** with only 45 percent respondents performing enhanced due diligence on PEPs at account opening stage.	**There was more focus on PEPs.** Eighty-one percent of respondents performed enhanced due diligence on PEPs at account opening stage.	**PEPs are now an area of focus for almost all respondents**, with 96 percent using PEP status as a risk factor and 88 percent monitoring PEPs on an ongoing basis.
Sanctions compliance	Not covered in the survey.	**Sanctions compliance is now a major challenge and source of AML investment** due to increased regulatory focus. However, 20 percent of banks did not have any procedures in place to update principal information for the purposes of sanctions compliance.	**Sanctions compliance remains a challenge**, with client screening seen as the most difficult area. Seventy-four percent of respondents identify all directors and controllers. Worryingly, only 50 percent use the new MT202COV SWIFT message.
Transaction monitoring	**Enhanced transaction monitoring systems was the main area of increased AML spending, but not universally.** Sixty-one percent of banks use internally developed systems, with 45 percent using those developed externally. However, 22 percent used neither.	**People are still the first line of defence in the fight against money laundering,** despite it being the greatest area of AML investment. 97 percent of respondents still relied primarily on their people to spot suspicious activity. Satisfaction with systems is 'neutral', at an average of 3.7 out of 5.	**Questions are starting to be raised about transaction monitoring.** Overall, respondents' satisfaction with transaction monitoring remains neutral, at an average score of 3.6 out of 5, but many regions are less satisfied than in 2007. **It remains the greatest area of AML spending.**
Risk-based approach	**Banks were adopting a risk-based approach.** Eighty-one percent of respondents adopted a risk-based approach at account opening stage.	**There was a broader acceptance of a risk-based approach.** Eighty-six percent of respondents used a risk-based approach to KYC activity.	**Taking a risk-based approach to KYC requirements is now almost universal.** Ninety-one percent do so at account opening.
Know Your Customer	**Banks increasingly understood the importance of AML compliance for existing and new customers.** Seventy-four percent of respondents remediated information gaps for existing customers, even if taken on before new KYC rules or guidance.	**Banks continue to use remediation programs to 'backfill' customer data.** There was a slight but not significant increase in the number of banks engaged in a remediation program, with 77 percent of banks having a remedial plan in place.	**KYC information is refreshed by almost all institutions, but not consistently across regions.** Ninety-three percent of respondents have a program in place to remediate information gaps, but the approach varies greatly. **FATCA is the greatest immediate KYC challenge.**
Regulatory approach	**The regulatory AML burden was acceptable but the requirements could be more effective.** Eighty-four percent of respondents believed the burden to be acceptable, but 54 percent felt that it could be more effective.	**There was broad support for regulatory AML efforts, but also more to do.** Ninety-three percent of respondents thought the regulatory burden was either acceptable or should be increased, however 51 percent said it could be better focused.	**Regulators are active, but banks want more collaboration and information.** Eighty-five percent of banks feel that the overall level of regulatory burden is acceptable, but many wanted more guidance and a collaborative approach.

Senior management focus squeezed by other priorities

Money laundering remains a significant risk and cost, and failure to have adequate AML programs presents a significant risk… but senior management interest is decreasing.

Although the costs of AML compliance continue to rise, the findings of our research reveals that the global financial crisis has moved AML down the senior management agenda. AML professionals will need to ensure AML remains on the top table in order to deal with significant change in the pipeline.

Only 62 percent of respondents cited anti-money laundering as a high profile issue for senior management, down from 71 percent in 2007

Whilst this may appear surprising, given that global regulators have been emphasizing the role of senior management for many years, the majority of the remaining financial institutions stated that AML was a moderately ranked issue in which senior management took some interest. Given the variety and severity of the issues facing management boards in the financial services community over the past three years, the slight fall in the perceived priority of AML is understandable.

The importance of AML to European senior management is falling faster than the other regions, with only 55 percent of respondents stating that AML was a high profile issue in which the main board of directors took an active interest (down from 70 percent in 2007). This may in part be due to the implementation of the EU Third Money Laundering Directive, leading to a temporary increased focus by senior management in 2007 before returning to a level comparable to that in 2004 (60 percent). Once policy and procedural changes had been implemented, the focus of senior management on AML may have lessened.

It is interesting to note that 96 percent of respondents working in the Central and South America and the Caribbean region cited AML as being a high profile issue in which senior management took an active interest. Approximately half of respondents' boards of directors in this region discuss AML issues on a quarterly basis, up from 40 percent in 2007.

This may be due to a combination of factors, including new money laundering cases in the region relating to narcotics trafficking and political corruption; more stringent requirements imposed on financial institutions in the region by their primary correspondent banks in the U.S. (some of which have been subject to AML enforcement actions); and a number of countries in the region being singled out recently by the Financial Action Task Force (FATF) for deficiencies in their approach to AML and counter-terrorist financing. Whatever the reason, AML has clearly leapt up the agenda in this region.

Conversely, only 50 percent of the financial institutions surveyed in the ASPAC region stated that AML was a high profile issue. This may be due to regulators being less active than those in other regions, with consequently lower levels of regulatory enforcement.

While 41 percent of respondents from the Russian, Baltic and Central Eastern Europe (CEE) region stated that AML was discussed on a monthly basis, 60 percent commented that AML was considered only a moderate profile issue in which the main board of directors took some interest.

Figure 1

Profile of AML at senior management level

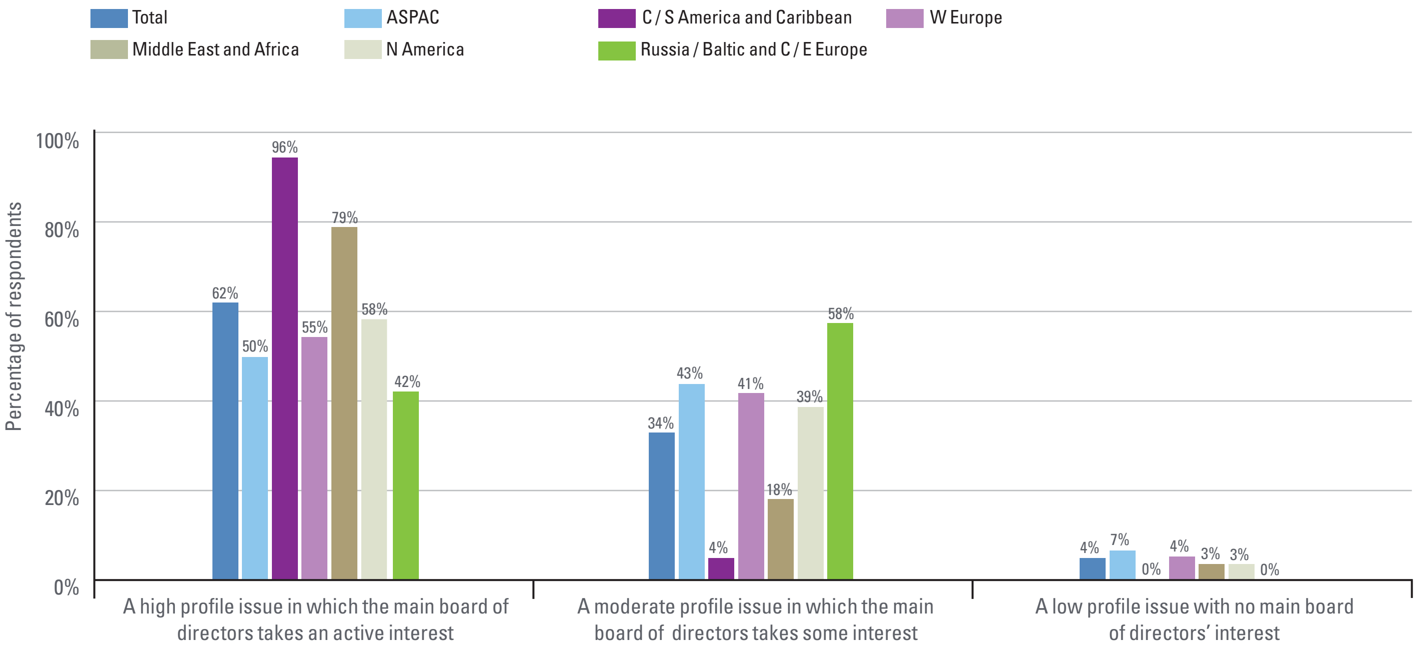
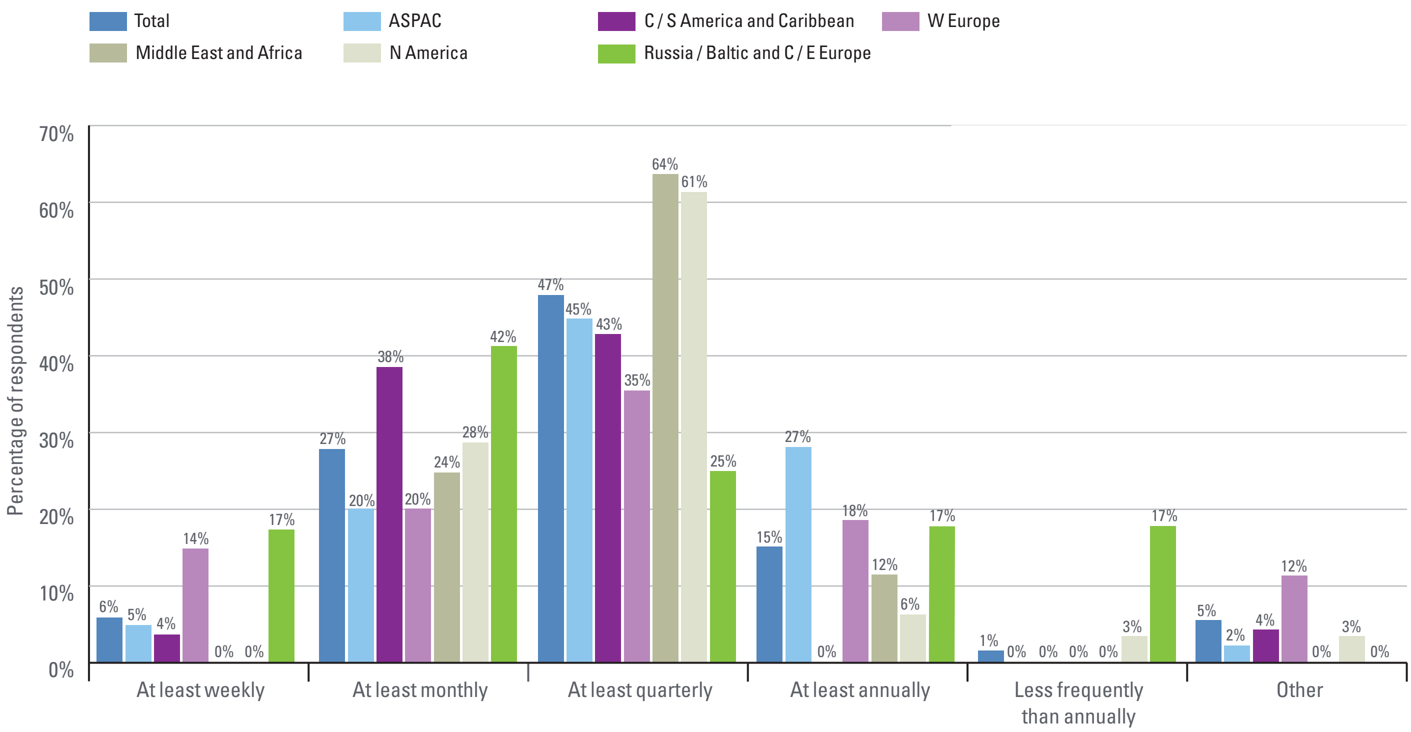


Figure 2

Frequency with which AML issues are formally discussed by the board of directors



Costs of AML compliance have risen by an average of 45 percent in the last three years, with more than 80 percent of respondents reporting a cost increase over that time

This rise in costs was reported across all regions, other than North America where only 64 percent of respondents reported an increase. Our Global AML survey has consistently shown an increase in AML costs, and there is no sign of respite for AML professionals with a mass of changes and new legislation on the horizon that will impact AML programs. AML will undoubtedly continue to be a high cost activity for the foreseeable future.

As in the previous two surveys, respondents cited enhanced transaction monitoring as the main reason for the increase in AML expenditure. In the ASPAC region, regulatory enforcement actions have centered on identified deficiencies in the reporting of suspicious activity, which may have led to a greater focus on this area. In the UK, however, we have noted a rise in the number of transaction 'look-back' reviews, primarily as a result of the extra-territorial reach of U.S. legislation and weaknesses in underlying KYC data highlighted following sanctions compliance investigations.

Interestingly, 'increased external reporting requirements to your regulator or external law enforcement agencies' was the second highest reason for increasing costs. This is a clear indication of the impact of a tightening regulatory regime faced by financial institutions.

'Anti-bribery and corruption activities' was introduced to the latest survey, immediately being ranked as the third largest area of expenditure. Unsurprisingly, a greater percentage of the respondents in Central and South America and the Caribbean as well as the Middle East and African regions considered this to be an area that has impacted the cost of their AML compliance. This may be as a result of the extra-territorial reach of, and the heightened regulatory expectation associated with, the UK Bribery Act 2010 and the U.S. Foreign Corrupt Practices Act (FCPA).

Costs have risen, but respondents have a track record of under-estimating future costs

Despite the overall increase reported, our research highlighted that many AML professionals around the world significantly under-estimate the future cost of AML compliance work.

In our 2007 survey, less than one-fifth (17 percent) of respondents predicted a rise of 51 percent of more in the following three years. However, in our latest research, 31 percent stated that their costs had actually risen by more than 51 percent in that period.

This trend was repeated between our first and second AML surveys in 2004 and 2007. In 2004, the overall prediction was of relatively minor AML cost increases over the following three years, with only fractionally more than one in five (21 percent) expecting a rise of 51 percent or more. Yet, in 2007, twice as many respondents (41 percent) reported that costs had increased by 51 percent or more since 2004.

The same trend is evident in the average increase in AML expenditure. In 2004, those predicting a rise in costs predicted an average rise of 43 percent, whereas the actual rise in our 2007 survey was 58 percent. In 2007, the prediction remained almost the same, with an average 40 percent increase expected. Our research shows that respondents were closer this time around, with the average increase being 45 percent in the last three years. However, the average prediction for the next three years has dropped to 28 percent.

With over three quarters of respondents predicting either no increase at all or an increase of less than 50 percent over the next three years, and only eight percent expecting an increase of more than 51 percent, it is likely that respondents have again under-estimated costs, especially when considering the volume of regulatory change in the pipeline. As business cases are presented to Boards, it is critical that AML teams provide realistic figures. Boards are generally not sympathetic to additional requests for funding when costs prove higher than predicted.

Our research highlighted that many AML professionals around the world significantly under-estimate the future cost of AML compliance work.

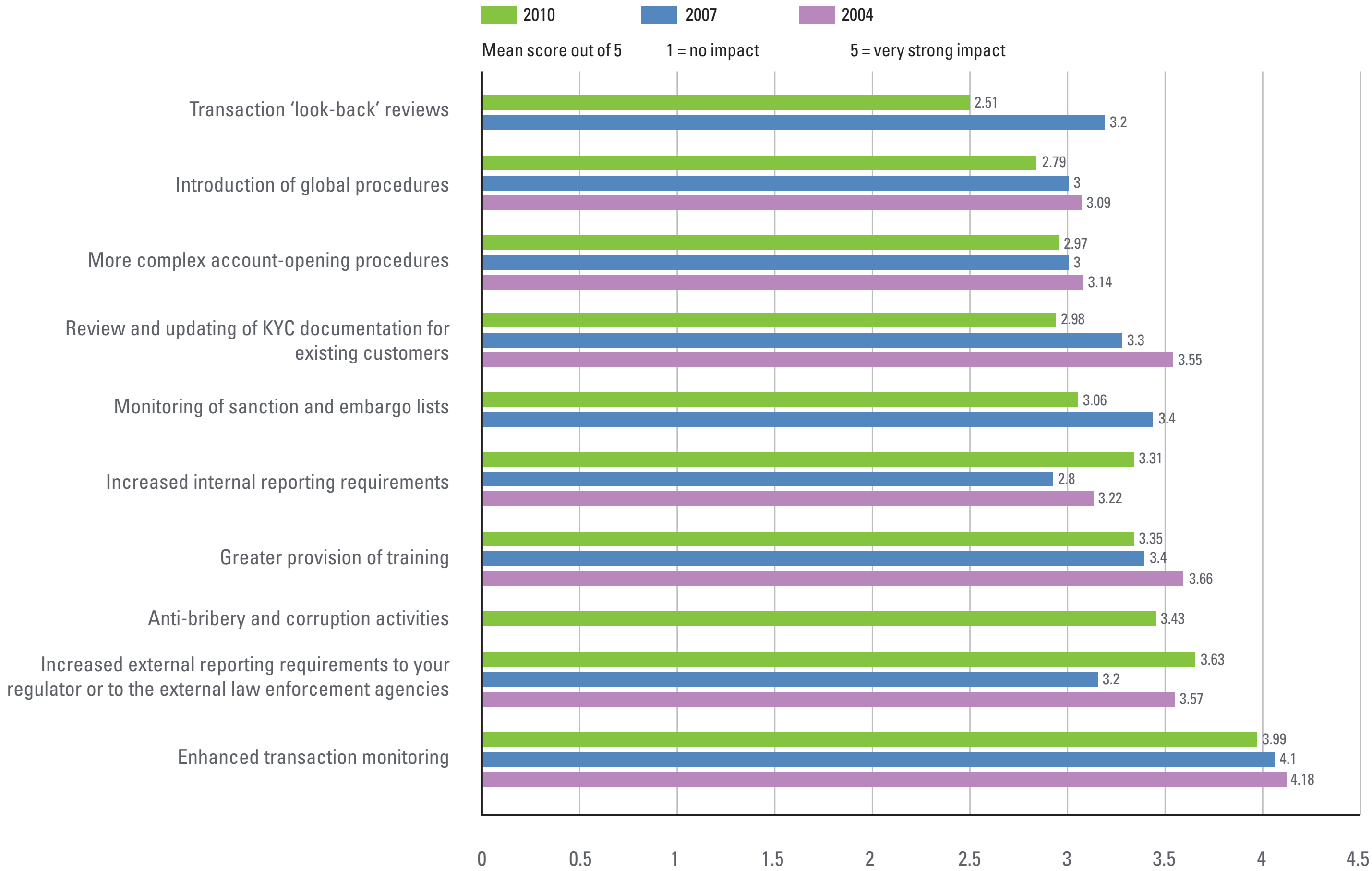
Figure 3

Respondents estimates of the average percentage increase in AML investment over the three periods: 2004-2007, 2007-2010, and 2010-2013

Note: 18% of respondents believed that there would be no increase in AML costs over the next three years.

Figure 4

Financial institutions' estimates of greatest AML investment over the last three years



> **"I don't feel that [outsourcers] would have a full understanding of our customer base."**
>
> KPMG Global AML Survey respondent

Only 10 percent of respondents have outsourced or off-shored AML functions, while almost 80 percent say they have not even considered doing so

This is interesting given that financial institutions anticipate the cost of AML compliance to continue rising over the next three years. It could be that there is a perception that any cost savings obtained through moving certain AML functions to a lower cost location will be negated by greater levels of due diligence being required to ensure that high standards of compliance are maintained. However, the primary reason for not off-shoring/ outsourcing AML functions is concern over sending confidential customer data overseas.

Those institutions that have off-shored or outsourced AML functions, in part or in full, often do so only once they understand how these other risks can best be managed. Solutions sometimes involve enhancements in data warehousing and transmission technologies, irrespective of where the information is maintained. Alternatively, a detailed risk assessment of the jurisdictions involved (whether it is the location involved in processing, the office that owns the relationship or the origination of the customer) may determine what data can and cannot be off-shored, or at least the extent to which regional 'hubs' can be deployed.

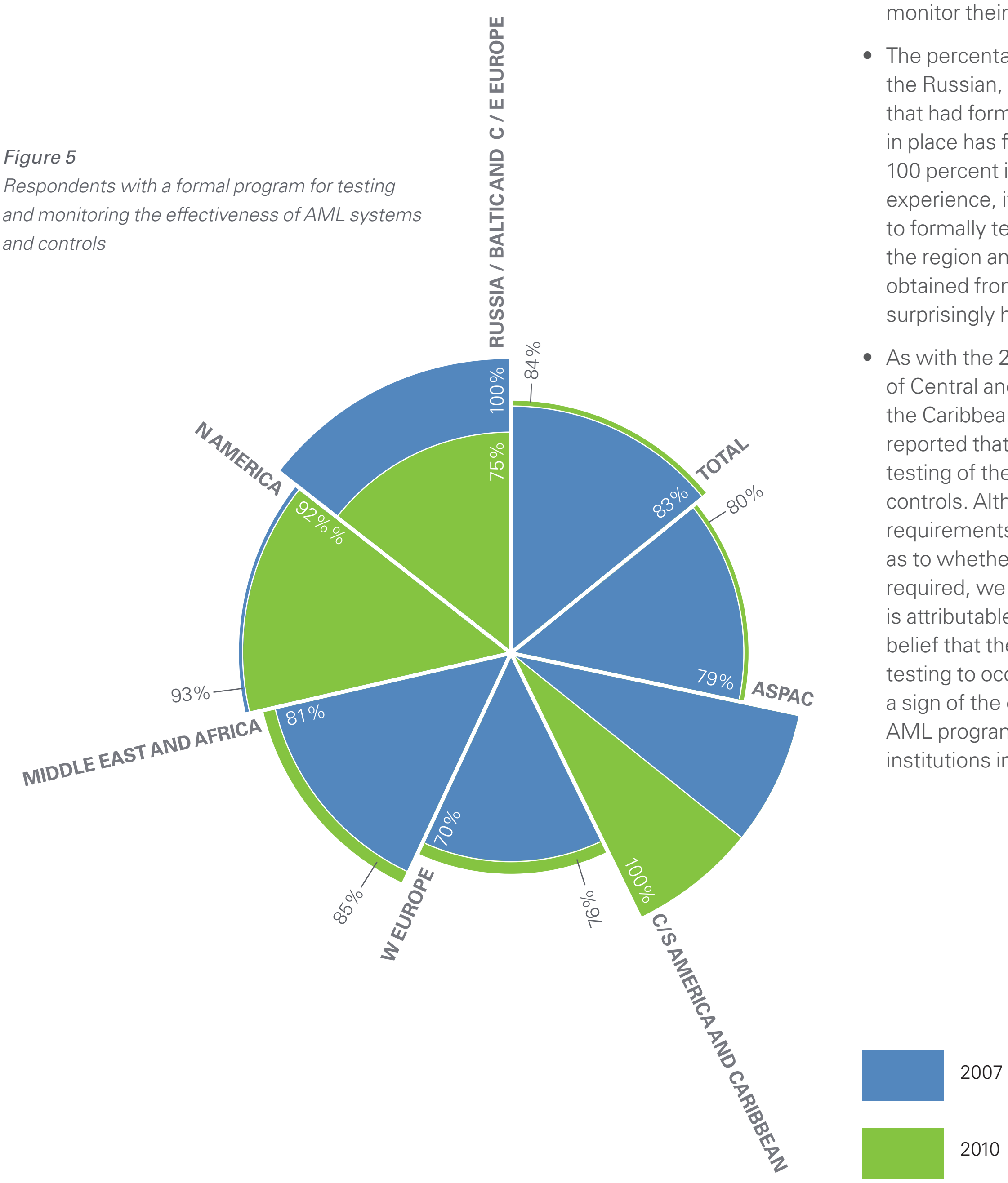
Of those financial institutions that have off-shored or outsourced, 68 percent have done so with the updating of sanction lists. No doubt as a result of concerns over confidential customer information, it is primarily the low risk AML activities that have been outsourced or off-shored.

Nearly one-fifth of financial institutions do not formally test and monitor the effectiveness of their AML systems and controls

This raises the question as to how financial institutions can gain comfort that systems and controls are operating as expected and therefore place reliance upon them. Globally, regulators are increasingly expecting banks to identify their own compliance issues as part of routine assurance testing, so banks are exposed if they don't have a robust program of testing.

Figure 5

Respondents with a formal program for testing and monitoring the effectiveness of AML systems and controls



While this finding is in line with the 2007 survey, there are a few points of particular interest:

- Eight percent of North American financial institutions stated that they do not undertake formal testing of their AML systems and controls despite such being a requirement of the U.S.A. PATRIOT Act.
- As with the two previous surveys the European figure appears low (albeit increasing from 2007) with only 76 percent of financial institutions reporting that they formally test or monitor their AML controls.
- The percentage of respondents within the Russian, Baltic and CEE region that had formal testing or monitoring in place has fallen to 75 percent from 100 percent in 2007. In our firms' experience, it is not general practice to formally test AML systems within the region and, as such, the results obtained from both surveys are surprisingly high.
- As with the 2007 survey, 100 percent of Central and South America and the Caribbean region respondents reported that they engage in formal testing of their AML systems and controls. Although local regulatory requirements within the region vary as to whether such testing is, in fact, required, we believe that the response is attributable to the respondents' belief that their regulators expect such testing to occur. We also take this to be a sign of the continued maturing of the AML programs maintained by financial institutions in the region.

What do we think?

Although senior management interest has waned, the fact that AML still ranks relatively highly on senior management's agenda is encouraging at a time when the primary focus for many banks has been their very survival. The regulators' continuing (and in some cases intensifying) focus on this issue means that those boardrooms where AML continues to have traction will be better positioned to deal with such scrutiny; those boardrooms where it no longer has that traction would be well advised to reconsider their approach.

For those boards who are engaged with AML, the challenge is how to improve the effectiveness of that engagement. Based on what we are seeing at our firms' clients, we believe this challenge is manifesting itself across three discrete areas within AML and Counter Terrorist Financing (CTF) frameworks:

The regulators' continuing (and in some cases intensifying) focus on this issue means that those boardrooms where AML continues to have traction will be better positioned to deal with such scrutiny; those boardrooms where it no longer has that traction would be well advised to reconsider their approach.

1. Signing-off higher risk relationships:

   At an operational level, senior management should be more actively involved in the decision-making processes with respect to the highest risk relationships, whether the decision is to undertake a new relationship or to maintain an existing relationship. Knowing when to obtain senior level sign-off and when to allow more expedited account opening is a dilemma for many clients.

2. Investing in systems and controls, both enhancements to existing arrangements and sanctioning new developments:

   A massive amount of money has been spent – and continues to be spent – on AML and CTF systems and infrastructure, from sophisticated screening and monitoring systems to expensive KYC remediation exercises where fundamental deficiencies in core processes have been identified. In these circumstances, it is both prudent and reasonable for senior management to ask whether (a) the metrics are in place to assess whether these investments are achieving the desired goals and (b) what arrangements need to be embedded to ensure that the outcomes of this sizable investment are robust and sustainable.

3. Engaging with regulators:

   There is an expectation that, as a result of a risk-based approach to AML and CTF, senior management will completely understand the key risks impacting their business and as such will be in a position to articulate to regulators the controls that are in place to mitigate these risks. Again, management must be provided with detailed metrics and management reporting with respect to the output of their institution's systems and controls to successfully engage with regulators on these issues. It is not practical for senior management to have a detailed knowledge of all the inner workings of the program, so they need effective assurance with alert mechanisms to understand where there may be problems.

It is not practical for senior management to have a detailed knowledge of all the inner workings of the program, so they need effective assurance with alert mechanisms to understand where there may be problems.

The scrutiny intensifies around Politically Exposed Persons (PEPs)

The focus on PEPs has intensified with recent events in the Middle East and North Africa; financial institutions find themselves in a key role regarding international financial crime initiatives. Firstly, momentum has been gathering in relation to global bribery and corruption programs, and secondly the Arab Spring uprisings have exacerbated this trend.

Of those financial institutions that have adopted a risk-based approach to KYC, 96 percent use PEP status as a risk factor (up from 81 percent in 2007)

Across all respondents, irrespective of whether they have adopted a risk-based approach to KYC, 88 percent said they had specific procedures for identifying and monitoring PEPs on an ongoing basis. This represents a continuing upward trend from approximately 71 percent in 2007 and only 45 percent in 2004.

More than a quarter of ASPAC respondents do not identify and monitor PEPs

Given the risks associated with PEPs, and indeed bribery and corruption as a whole, it is interesting that ASPAC lags behind other regions, with only 73 percent of respondents identifying and monitoring PEPs. This is significantly higher, however, than the 42 percent reported in 2007. Our member firms' experience suggests this is due to ASPAC financial institutions focusing primarily on screening individuals or organizations identified by local regulators, rather than more subjective PEPs.

There has also been a substantial increase within Europe in the proportion of financial institutions applying specific procedures to identify and monitor PEPs, from 65 percent in 2007 to 94 percent in 2011. This is likely to be due to the EU Third Money Laundering Directive, which requires financial institutions to 'conduct enhanced ongoing monitoring of the business relationship'[1] in respect of transactions or business relationships involving PEPs.

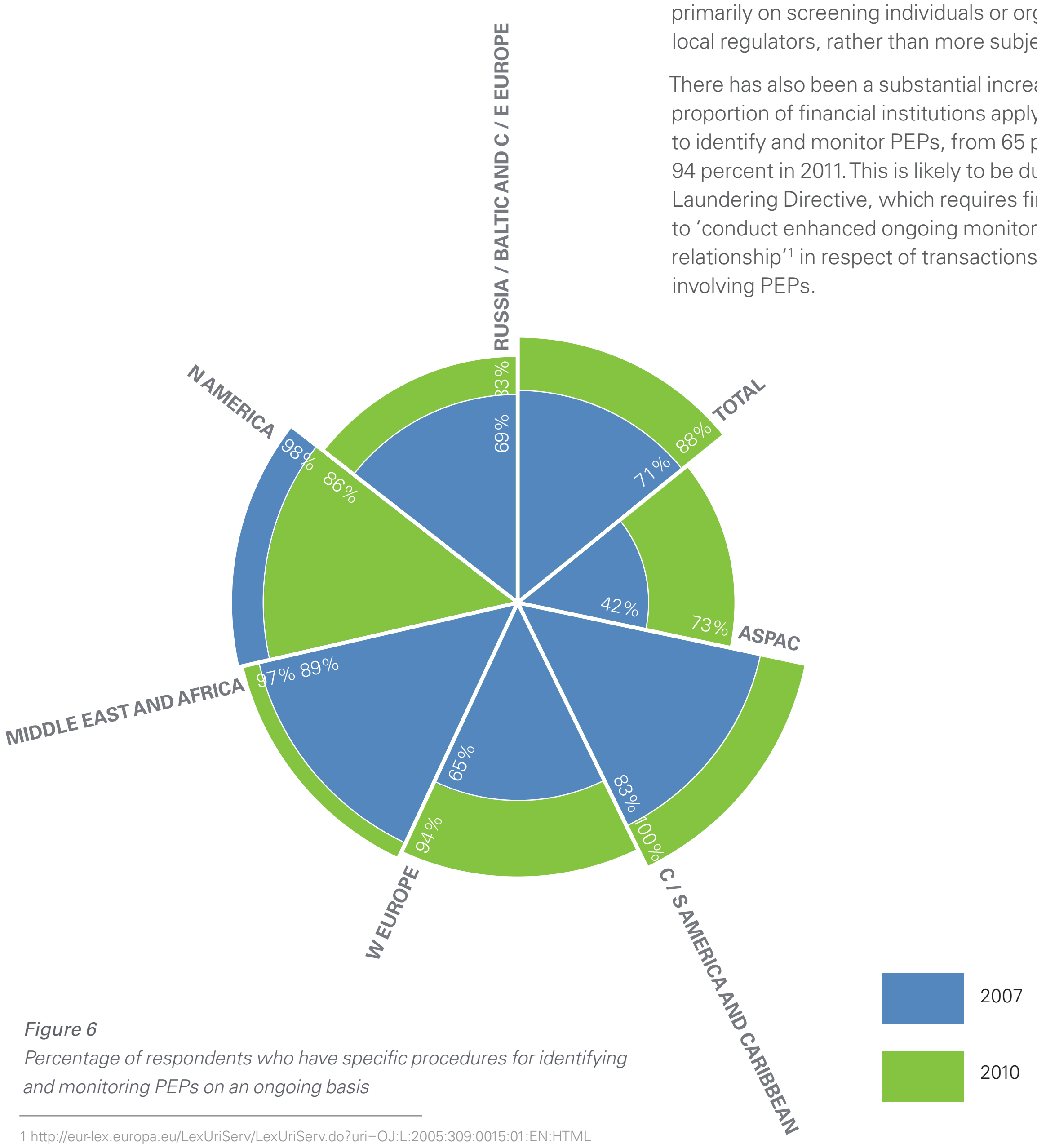


Figure 6

Percentage of respondents who have specific procedures for identifying and monitoring PEPs on an ongoing basis

1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

"Governments or states should provide a list of people that are politically exposed."

KPMG Global AML Survey respondent

The identification of foreign PEPs remains a key requirement under the U.S.A. PATRIOT Act. While the identification and risk mitigation processes associated with PEPs remains a high priority, only 86 percent of North American financial institutions reported they had specific procedures in place to identify and monitor PEPs.

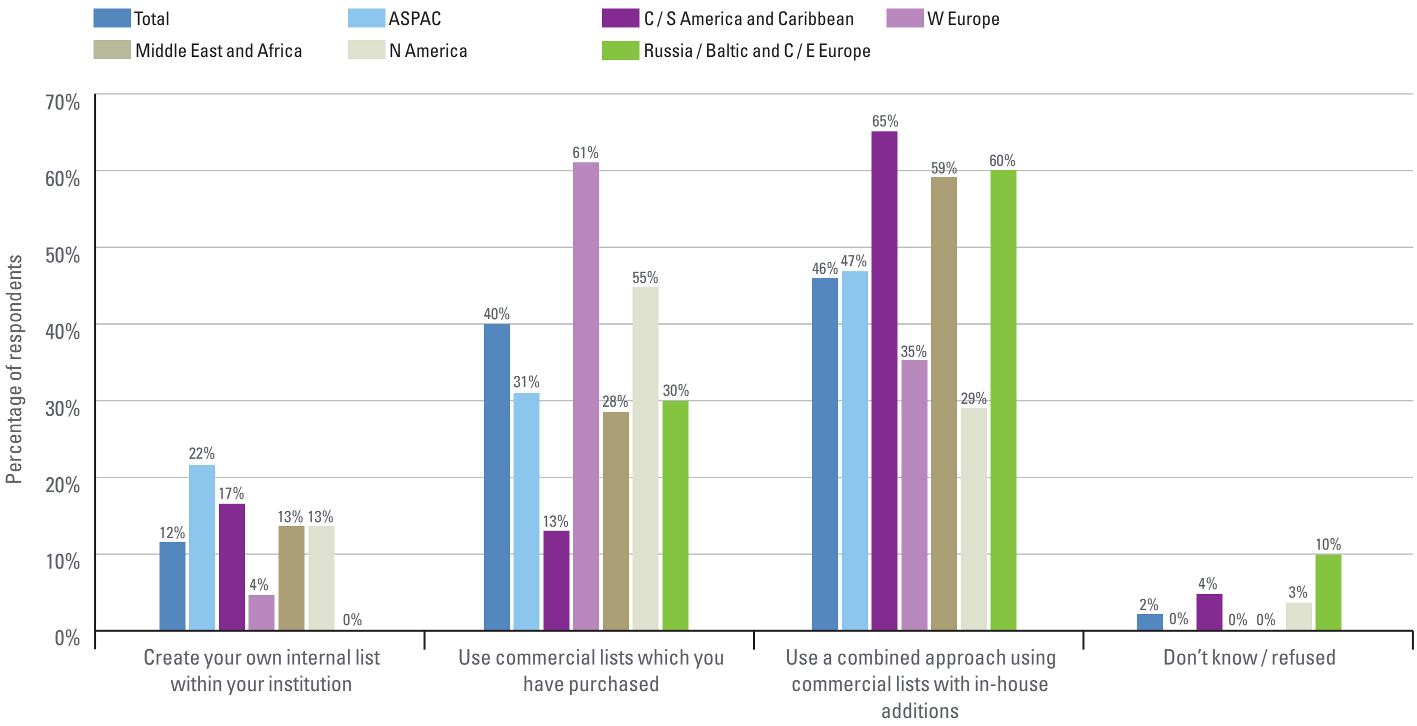
A possible explanation for this is that, as domestic PEPs are not captured by U.S. PEP regulations, U.S. financial institutions with a purely domestic client base may not have developed processes to identify and review PEPs, whether foreign or domestic. Going forward, it will be interesting to see if regulatory authorities change their position on excluding domestic PEPs from heightened identification and review requirements, especially as international AML bodies consider recommending that domestic PEPs be treated in a manner similar to foreign PEPs.

Sixty-one percent of European and 55 percent of North American financial institutions use commercial lists to identify PEPs

The remaining regions tend to use a hybrid approach, amalgamating commercial lists with in-house additions. One explanation for this approach, particularly within the ASPAC region, is the release by regulators of their own lists of undesirable organizations. As such, financial institutions would need to incorporate their regulators' lists into the commercially available PEP lists.

Figure 7

Approach by financial institutions to identify PEPs



What do we think?

Senior management must understand the risks associated with providing services to PEPs and must be able to demonstrate active engagement, whether in the context of setting the risk appetite for the organization or formally and affirmatively approving these highest risk relationships.

In our firms' experience, banks are generally able to identify whether a customer might be a PEP (or are at least introducing systems or using vendor screening packages that might enable them to do so). However, they are less able to use this information on an ongoing basis to manage the risk that their institution may be used to launder the proceeds of bribery, corruption and other financial crimes such as tax evasion.

As the ongoing monitoring of these relationships is absolutely critical, it is essential that financial institutions are equipped with the appropriate resources to manage the risk. That does not only mean technological solutions, but also the provision of training and tools to assist those in the 'front office' who are best placed to identify riskier transactions, such as relationship managers and private bankers.

"The definition of PEP's varies from country to country… so we use an international negative list."

KPMG Global AML Survey respondent

The Arab Spring and its impact on PEPs

Since this survey was commissioned, uprisings dubbed 'the Arab Spring' have occurred across the Middle East and North Africa. Since December 2010, when the first uprising started in Tunisia, attention has focused on the activities and actions of the ruling parties within the affected countries. These factors have led to a greater focus among financial institutions on PEPs residing within the affected jurisdictions, and the possibility that they could be involved in, or assisting in, the movement of assets out of those countries.

As a consequence, and particularly in relation to Libya, a number of PEPs have been re-classified as sanctioned individuals due to the closeness of their association with the respective regimes. Furthermore, any entity under the control of a newly sanctioned individual has also been reclassified as a sanctioned entity, due to the potential for it to be a source of funding for the relevant regimes.

Effective management of PEPs has been shown to be particularly important given the Arab Spring's impact on AML programs as PEPs become either *persona non grata* or sanctioned individuals overnight. Scrutiny and comment have focused on who was dealing with these PEPs, why, and what transactions they should have identified as potential corruption. In the absence of a robust process for ongoing review of PEP relationships, firms may be unable to defend themselves against allegations of doing business with allegedly corrupt dictators.

In addition, the UK Financial Services Authority's (FSA) recent themed review of PEPs identified that UK firms have made little progress in their handling of PEPs since the FSA found them to have laundered USD1.3 billion of funds stolen by General Abacha from Nigeria's coffers. It seems that there is still much to do to ensure that this high risk category of customer is effectively managed.

Image attribution: Author Jonathan Rashad, 2011 – released under the Creative Commons Attribution 2.0 Generic license.

Sanctions compliance remains a challenge

"It would be nice to align international sanctions as the EU is issuing sanctions as well as the UN which causes duplicate entries in the systems, therefore creating more work unnecessarily."

KPMG Global AML Survey respondent

Sanctions compliance has attained a high profile in recent years as governments' attempts to focus their efforts on preventing terrorist financing and Weapons of Mass Destruction proliferation have led to a number of high profile cases.

The U.S. Treasury Department's Office of Foreign Assets and Control (OFAC) has been particularly active in this area. Due to the extra-territorial application of U.S. treasury sanctions, a number of non-U.S. financial institutions have incurred heavy fines, the largest to date being USD536 million in December 2009.

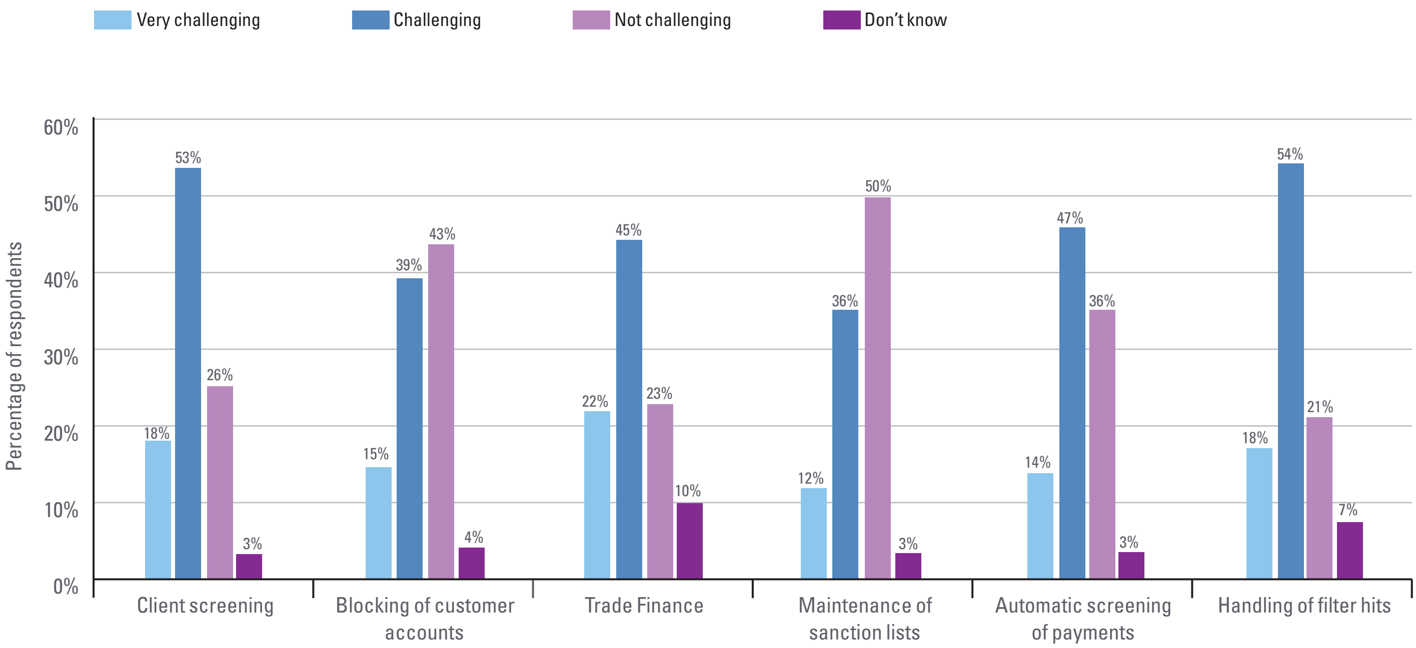
More than 70 percent of respondents find client screening and the handling of filter hits either challenging or very challenging

This is consistent with our firms' experience and the nature of work we have undertaken within the last three years. As sanction screening is undertaken in 'real time', with transactions held until potential 'hits' are investigated, financial institutions are confronted with a number of difficulties.

The underlying issue regarding sanction screening lies with the quality of customer data maintained by financial institutions. Poor or incomplete data may result in more 'hits' being generated, as well as difficulties in eliminating false positives.

Furthermore, customer data is often held on several systems, all of which may need to be screened. In many instances this may be as a result of each business unit having its own system, or it may be a consequence of historical acquisitions where the acquired entity's customer data is not migrated onto a system shared with the acquirer.

Figure 8
Difficulties faced in the area of sanction compliance



FATF Special Recommendation VII (FATF VII) is not fully in place globally, although 84 percent are compliant

North American respondents appear to be furthest behind in complying with FATF VII, which requires complete originator information to be included in wire transfers. Eleven percent of North American institutions (all of which are based in the U.S.) do not include originator information within their SWIFT messages. Furthermore, 22 percent of North American respondents (all but one based in the U.S.) do not screen incoming messages for completeness. This is surprising given the relative maturity of their sanctions screening processes and how active OFAC has been within the sanctions arena. It is particularly interesting given that the U.S. Bank Secrecy Act (BSA) requires that all financial institutions located in the U.S. and transmitting USD3,000 or more must include both originator and beneficiary information in the transmittal order.

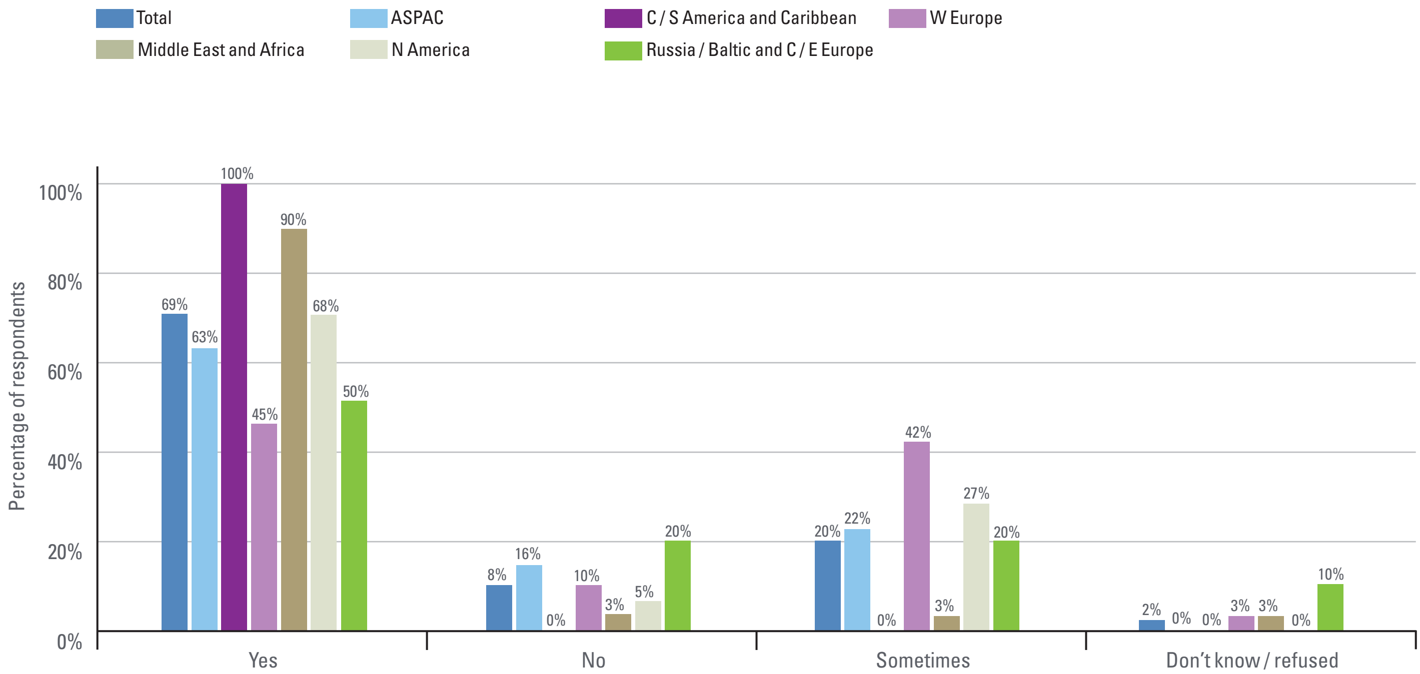
Only 45 percent of European financial institutions would stop a payment if the incoming SWIFT message was incomplete

As financial institutions need to know both parties to a transaction to comprehensively screen a payment, some may find this statistic concerning. However, it is worth noting that the requirement under the EU Third Money Laundering Directive is not to stop each payment, rather it is to monitor them to identify when there is routinely missing information from a particular bank.

Across all regions, of those financial institutions that do not currently stop messages with incomplete originator information, and hence the associated payment, only 25 percent planned to do so within the next year, whilst 67 percent had no plans to stop such messages in the future.

Figure 9

Percentage of financial institutions that stop messages with incomplete originator information



There is only variable use of MT202COV

The screening of SWIFT messages for completeness, and rejecting those that are incomplete, poses challenges given the large volume of messages that must be reviewed. It is especially difficult where the financial institution holds correspondent accounts and is acting only as an intermediary. In such situations, key information on the originator and the beneficiary may be missing.

To help overcome this weakness, the new MT202COV message was implemented on 21 November 2009, containing mandatory, standardized originator and beneficiary data fields.

Only 50 percent of respondents use the new MT202COV SWIFT message

The main user was the Middle East and African region, with 70 percent of respondents doing so. This comes as no surprise given that 90 percent of respondents within this region said they stop SWIFT messages with incomplete originator information.

Of those respondents that did use the new MT202COV message, only 34 percent stated that it was used in all instances where a cover payment was required.

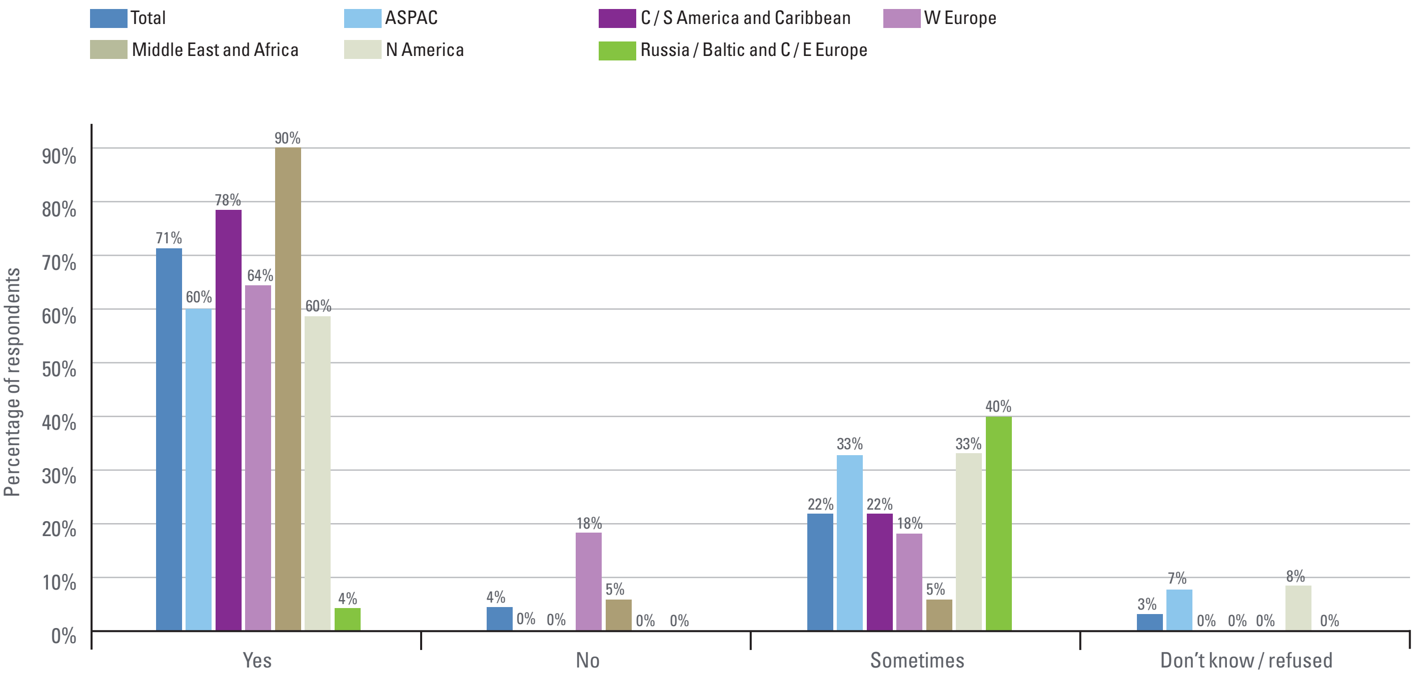
Only a quarter of European financial institutions stated that they always use the MT202COV, with a further 10 percent using it most of the time. As a result, when a cover payment is made, the majority of European financial institutions will not provide details of the originating and beneficiary parties to their correspondent banks, thus preventing the latter from fulfilling their sanctions screening obligations. However, of the banks surveyed with over 10 million customers, from where the majority of payments will originate, 75 percent use MT202COV. This compares to only 41 percent of banks surveyed with less than 5,000 customers.

"We are currently making investments to improve to a system that's capable of fuzzy logic and risk profiling."

KPMG Global AML Survey respondent

Figure 10

Percentage of financial institutions that would stop MT202COV messages with incomplete information



Twenty percent of European institutions do not screen incoming MT202COV messages for incomplete information; of those that do screen, 18 percent would not stop a payment if the MT202COV was incomplete

This may be expected given that the MT202COV is not yet in full use. We would expect to see this percentage rise as more institutions migrate to the new message type.

This finding may also be directly linked to how the initiative is being policed by various regulators around the world. More than two-thirds (69 percent) of respondents stated that regulators have examined their correspondent banking business lines. The corresponding percentage in Europe is comparatively low at 49 percent, in contrast to North America at 76 percent.

While the key to sanctions screening may be the quality and completeness of information, and measures such as the MT202COV are being implemented to improve this, it appears that not all financial institutions are amending their practices. If money laundering and terrorist financing are to be prevented, ensuring that all payments are transparent is absolutely essential. Financial institutions need to realise this and amend their practices accordingly.

What do we think?

Violations of sanctions laws have, to date, resulted in the largest regulatory fines. Our firms' clients, irrespective of where they are headquartered, are genuinely nervous of the U.S. regulators and often refer to sanctions compliance as a 'nuclear' area – an area that could bring the bank down. Unlike AML, sanctions compliance is a strict liability environment, where processing one payment in violation of the sanctions laws has the potential to lead to serious consequences.

As our results show, sanctions screening to date has focused almost exclusively on screening official lists. Knowledge of this fact, coupled with the publicity surrounding U.S. enforcement action means those seeking to evade sanctions will inevitably adapt their approach to circumvent these controls. It will become increasingly important to screen against lists containing relevant geographic indicators such as cities and ports, particularly when dealing with trade finance, and especially where transactions involve a U.S. nexus which gives rise to OFAC compliance obligations.

Surprisingly, 50 percent of respondents said that list management was not challenging. Given the noise that usually surrounds the lists issued by the authorities, the duplication of names on different lists and the perennial concern about the amount of identifier information included in such lists, we would have expected this to have been much lower. Many of our firms' clients struggle to get new lists uploaded within 24-48 hours of them being issued, as regulators and issuing authorities expect.

Regulators have become more risk-based in this area over the years, but firms spend disproportionate amounts screening customers and payments to ensure that payments representing hundredths of one percent of the total volume cannot pass through the system. Banks are duplicating screening – with the sending and receiving of bank screening payments and being unable to rely on each other or any central clearing house. Tens of millions are spent on this area by banks to try to avoid the hundreds of millions in fines, as well as the massive remedial work and look-back exercises that follow an enforcement action. Whilst this is a necessary evil, the challenge for the banking sector will be how to combine forces to ensure a more efficient framework going forward.

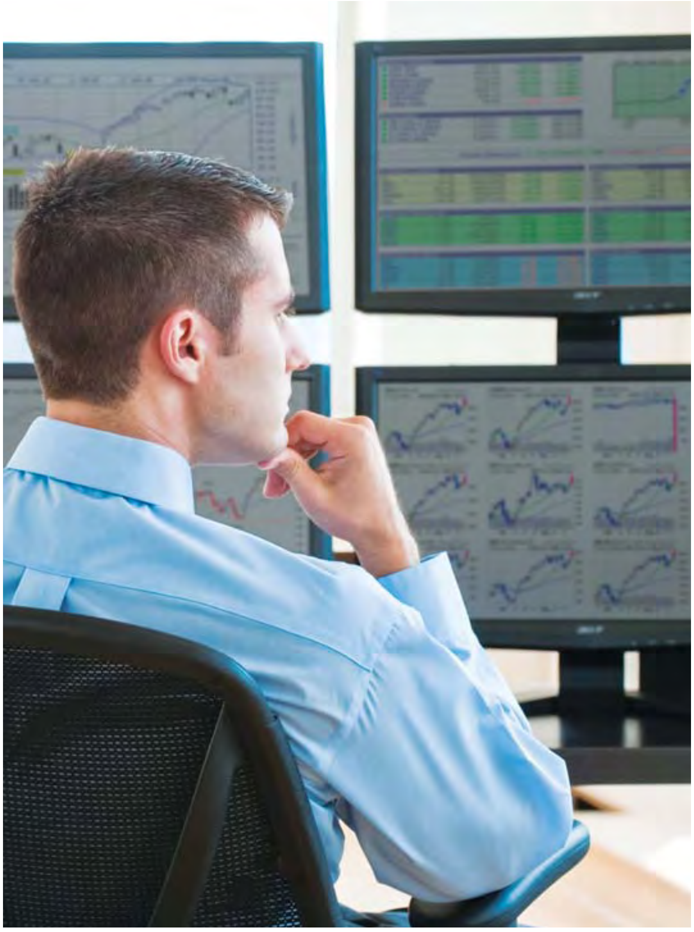
In this environment, it is not surprising that firms have focused first on ensuring effective screening of payments, before fully implementing FATF VII or looking for missing information in incoming messages. There is a sense of 'getting your own house in order', before tracking others in the market that are not providing the necessary information for screening. The effectiveness of this screening is reduced, however, if not everyone is doing the same. The variable use of the MT202COV message is a case in point, as without it, correspondent banks are blind to the information that they have spent huge amounts of money trying to screen.

In addition, it is increasingly important that banks can identify attempts to circumvent their controls, especially where payments (inbound or outbound) have been rejected or declined. We see the development of solutions to identify re-submitted payments, as well as evidence of payment stripping as the next logical evolution in sanctions screening.

In moving to such solutions, institutions need to consider how these controls will interact with monitoring programs to identify adherence to FATF VII, and Suspicious Activity Reporting (SAR) reporting obligations when issues are identified.

Sanctions compliance is a strict liability environment, where processing one payment in violation of the sanctions laws has the potential to lead to serious consequences.

Questions are starting to be raised about transaction monitoring



"Increase [monitoring systems'] ability to communicate with other standard banking systems. It is a struggle to get the systems to talk."

KPMG Global AML Survey respondent

A key aspect to tackling money laundering and terrorist financing is to undertake 'ongoing monitoring' of the business relationship with each customer. This means not only the monitoring of all transactions involving the customer to ensure that they fall within expectations, but also ensuring that all KYC documentation is accurate, complete and up-to-date.

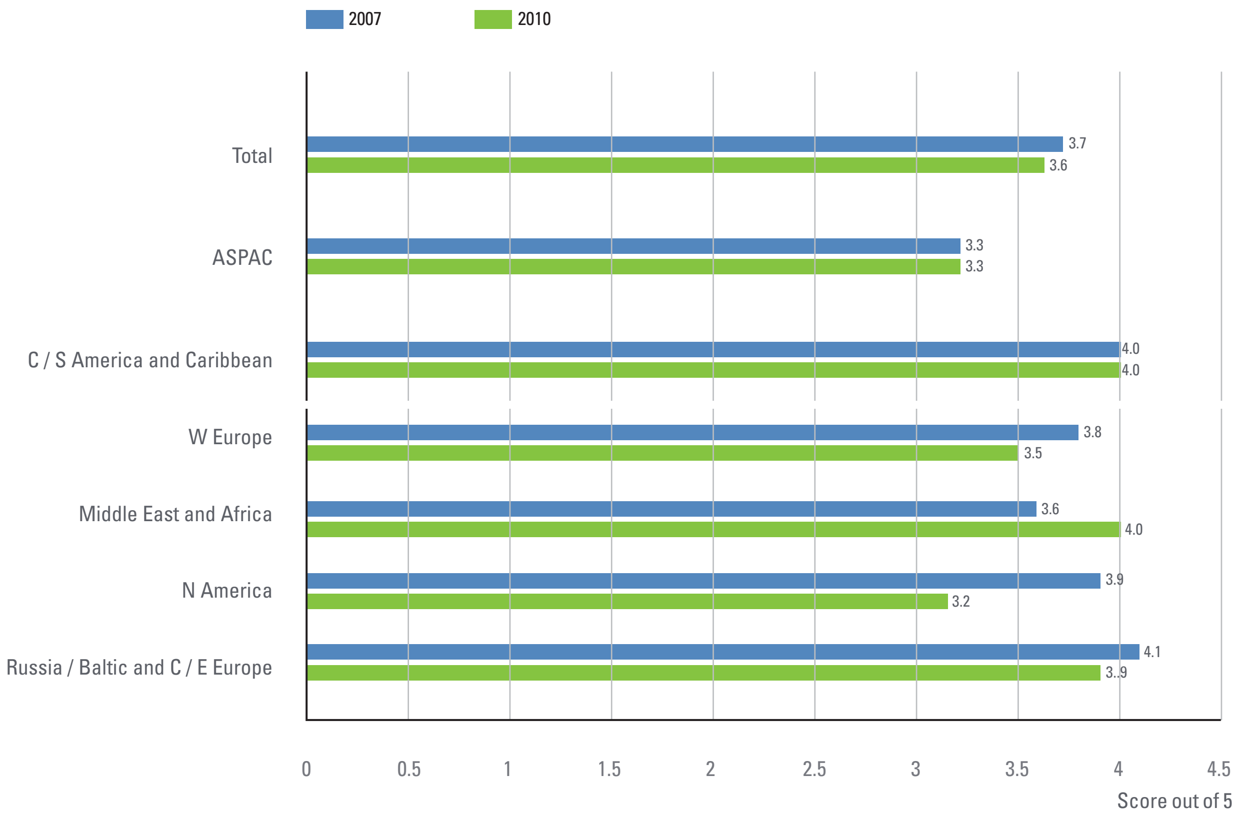
The monitoring of transactions to ensure that they are consistent with the institution's understanding of the customer has been the cornerstone of financial institutions' AML systems and controls, along with robust account opening procedures, for much of the last decade. This is reflected in costs incurred by institutions in delivering against this regulatory objective: since the survey began in 2004 transaction monitoring has been the largest AML compliance cost driver.

North American financial institutions are the least satisfied with their monitoring systems and controls

The fall in North American respondents' satisfaction from a score of 3.9 to 3.2 out of 5 is consistent with our experience, particularly with respect to securities firms and financial institutions that carry on non-retail business. Here, a common complaint among AML professionals is that traditional AML surveillance of institutional customers is ineffective.

The level of investment in transaction monitoring as well as systems requiring complex rules or algorithms to operate, or which are not considered to be 'user-friendly', may also impact buyer satisfaction.

Figure 11
Respondents' satisfaction with their transaction monitoring systems



"We have no interaction between our monitoring system and the customer's risk rating so, what I've already recommended is to find a new vendor."

KPMG Global AML Survey respondent

Less than one-third of respondents are able to monitor a single customer's transaction and account status across several countries

Although low, this represents an increase from just over one-fifth in 2007. The Central, South America and the Caribbean region leads the way in cross-border monitoring, with 57 percent of respondents being able to monitor a single customer's transactions and account across multiple countries. This contrasts with only nine percent of ASPAC respondents.

Implicit in the 'ongoing monitoring' requirement is the expectation that the Customer Due Diligence (CDD) performed – and the corresponding data gathered – will be used for the purposes of transaction monitoring. In larger, more complex and often multinational financial institutions, the success of a transaction monitoring system may be predicated on collating disparate information on a customer that is scattered across the organization.

The inability of a financial institution to monitor transactions across different countries calls into question how they are able to manage the expectations of regulators in whose jurisdictions they operate. Moving to a position in which a financial institution can fully understand and monitor its customers' transactions will facilitate the identification of unusual transactions or behaviors. We note that globally institutions are starting to look at their AML tools to understand how they can be leveraged for the introduction of FATCA in 2013 and 2014. While the FATCA regulations are not yet known, a single view of a customer's transactions across the Foreign Financial Institution may be a desirable component of the institution's FATCA approach. As the FATCA rules become clearer we anticipate, therefore, that the number of institutions able to monitor a single customer's transactions cross-border will increase.

"[Transaction monitoring systems could be improved by] extending the systems to all business activities across all countries, which is not currently the case."

KPMG Global AML Survey respondent

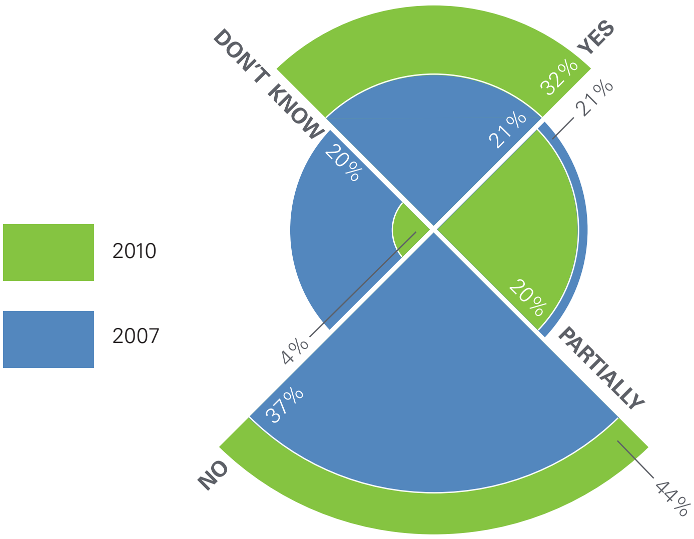


Figure 12

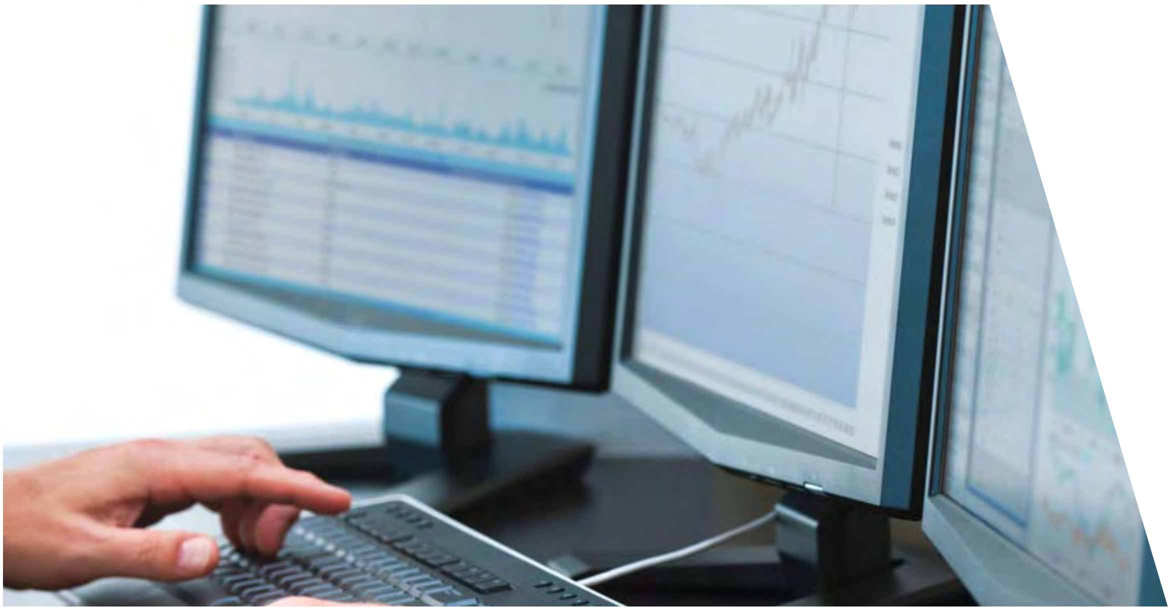
Capability of financial institutions to monitor a single customer's transactions and account status across several different countries

"We have a few monitoring systems which would be improved if we went through one system."

KPMG Global AML Survey respondent

"[It would improve monitoring systems] to be able to group relationships such as an individual person and that of an owner or director of a business."

KPMG Global AML Survey respondent



What do we think?

The identification of a customer is only one part of the AML risk management 'toolkit'; ongoing monitoring against this CDD is also vital. Unfortunately, our firms' are seeing that few clients and their systems are able to use the data collected at on-boarding for monitoring purposes, at least at the moment. As a result, KYC (or CDD) and transaction (or activity) monitoring arrangements are likely to continue as separate and distinct activities, undermining the effectiveness of this key requirement.

This principle also applies to wider risk management arrangements. Ongoing risk assessment should include intelligence generated internally as well as externally, and a key source for this data is monitoring tools and activities. The expectation of many regulators is that institutions can (and are) using information from monitoring to validate, calibrate and inform the identification of riskier parts of the business (at an enterprise level) and customers, products and services (at an operational level).

Our firms' clients are increasingly moving away from automated transaction monitoring in areas where the volumes are lower, and the effectiveness of automated monitoring is unproven. It is important, though, to have a documented justification for doing so, and to be able to articulate how the risk is being managed, for example by enhanced staff training, manual transaction reviews and restrictions on higher risk activity such as third party payments.

"We should collect more data and keep the records of the customers longer so that we can monitor the history of transactions to establish the trend and detect any irregularities."

KPMG Global AML Survey respondent

Know Your Customer data is not refreshed consistently

The second element of the 'ongoing monitoring' requirement is the need to keep relevant KYC data items up-to-date. Without up-to-date data, banks cannot understand their customers, nor screen a company's principals effectively against sanctions lists.

Almost one in five North American institutions has no program to refresh KYC on an ongoing basis

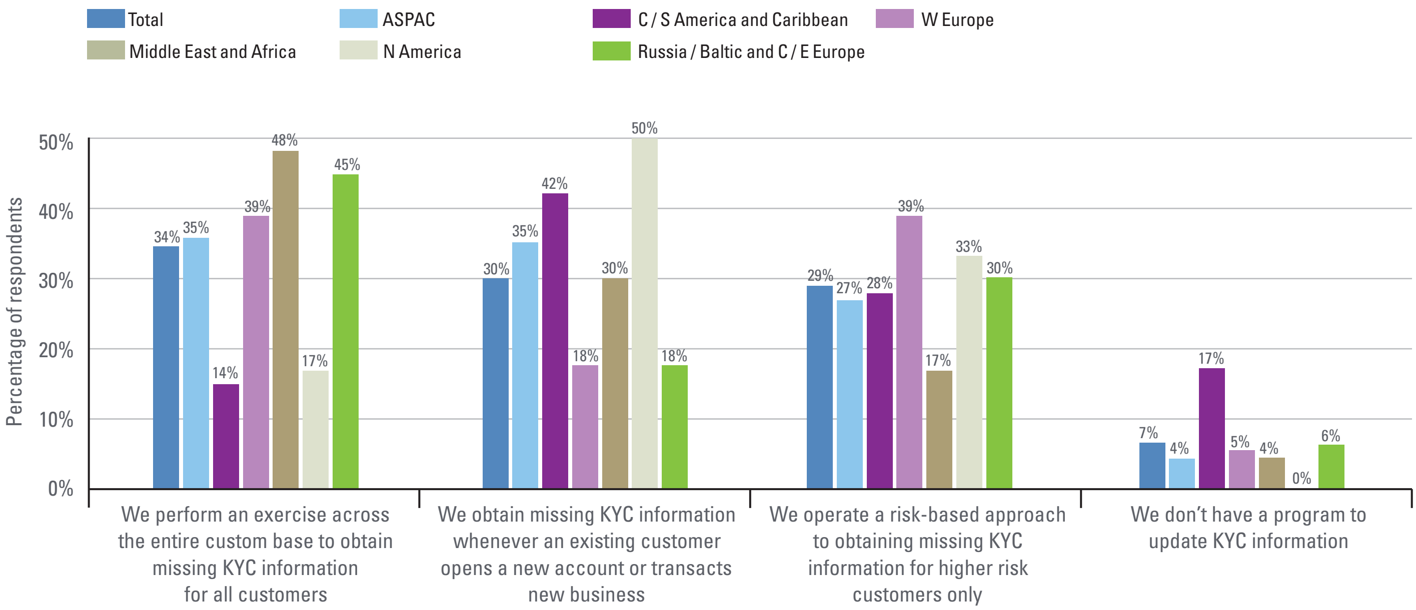
This may be due to financial institutions in the region placing a greater emphasis on AML transaction monitoring, rather than refreshing or remediating gaps in a customer's KYC information.

Conversely, almost all (96 percent) European financial institutions have a remediation program in place to update KYC information for their customers. This represents an increase from 73 percent in 2007. It is possible that this increase is, in part, a consequence of the investigations initiated by law enforcement and other regulatory agencies in relation to alleged weaknesses in sanctions compliance. Quite often, these investigations have drawn attention to significant gaps in the KYC information maintained by financial institutions. In these circumstances a remediation program is required to satisfy senior management, as well as the authorities.

Perhaps the greatest immediate challenge for those working in this sector, however, is that presented by FATCA. Although this legislation has its roots in tax avoidance strategies, the ability to identify relevant U.S. persons and parties for reporting purposes is likely to hinge on the KYC arrangements that are already in place. The fear is that enhancements will be required in order to deliver against these requirements, both in terms of the systems and controls used to consolidate relevant KYC information, as well as gaps in the information currently maintained (particularly if institutions need to be able to identify 10 percent shareholders or other beneficial owners in all relationships). AML professionals are likely to find themselves responsible for delivering these enhancements and remediation exercises, even though the legislation relates to tax. Indeed, European institutions that are already undertaking a KYC remediation exercise may find themselves contacting their customers again, specifically in light of the requirements of FATCA.

Figure 13

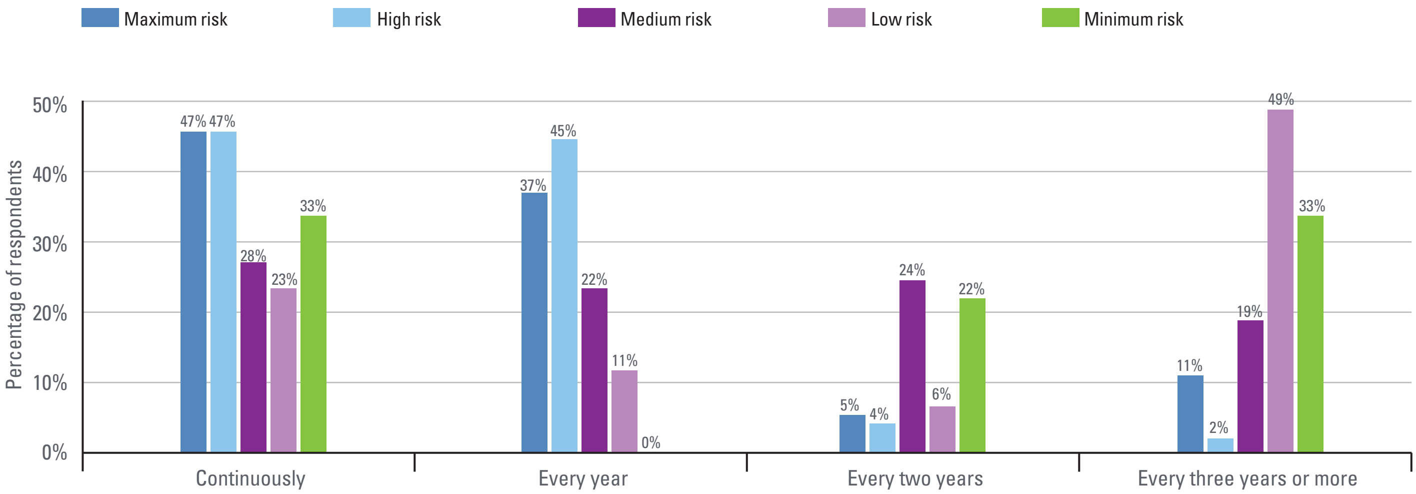
Approach taken by respondents in updating KYC information for existing customers



"We need country specific KYC requirements to reflect the reality on the ground. Every country has a different set up."

KPMG Global AML Survey respondent

Figure 14
Frequency of KYC review based upon customer risk rating



More than half of Central, South American and Caribbean financial institutions stated that they review KYC 'continuously' irrespective of the customer's risk rating

One explanation for this result may be due to financial institutions within this region not undertaking a truly periodic review of KYC data, but instead making changes to customer data on an ad-hoc basis.

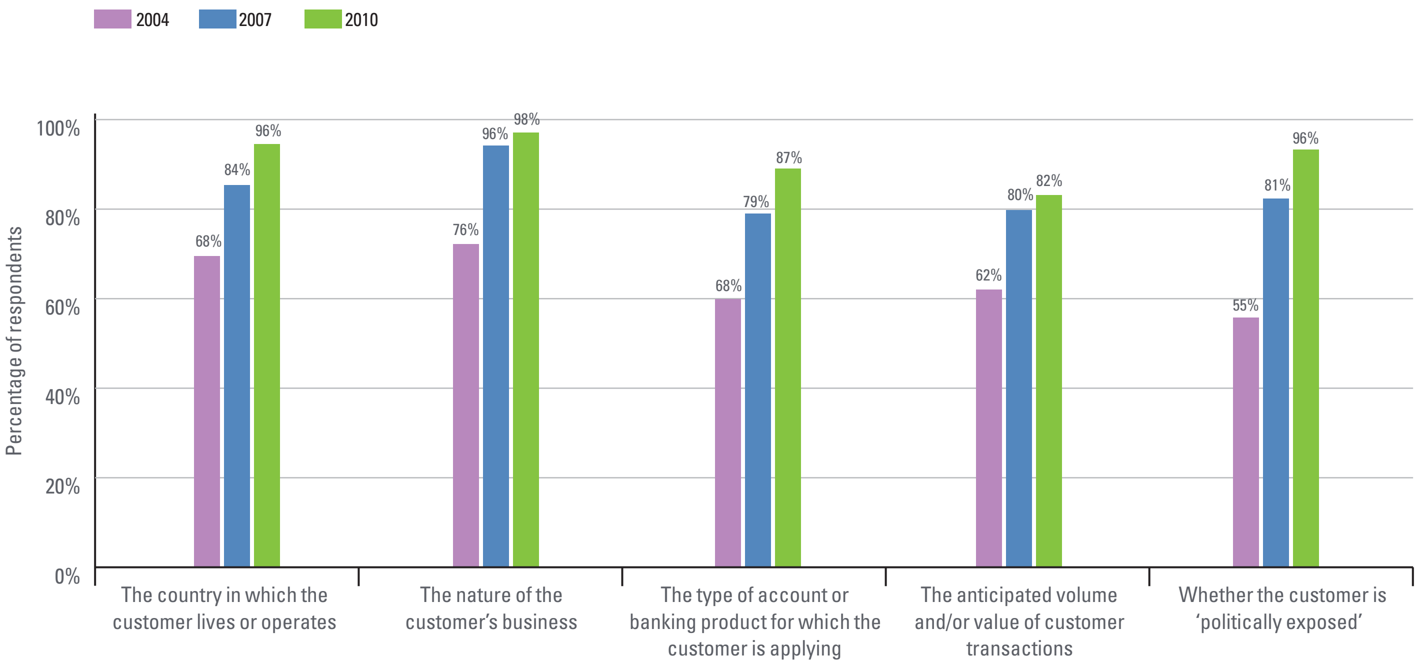
As the frequency by which a KYC review is undertaken generally depends upon the risk rating assigned to a customer, it is essential that financial institutions review risk ratings on a regular basis. Incorrectly classifying a customer as low risk impacts not only the timing of a review, but may also affect the number of directors, controllers and ultimate beneficial owners for which KYC is undertaken.

" A lot of the requirements for KYC information are not applicable to private institutions. We need more options and coordination in the requirements and more understanding of each area covered."

KPMG Global AML Survey respondent

Figure 15

Factors taken into account by respondents when using a risk-based approach at the account opening stage



Only two-thirds of ASPAC respondents use variable factors when assessing customer risk at the account opening stage

An ability to utilise data gathered for the purposes of CDD is critical. Since our first survey in 2004, there has been a significant rise in the use of a wide range of factors to assess the risk of a potential customer, in the context of the account opening process. Since our second survey in 2007, the proportion of institutions using the country in which the customer lives, the type of product for which the customer is applying, and whether the customer is a PEP, has increased by approximately 10 percent. However, the number of financial institutions using variable factors, such as the anticipated volume and / or value of customer transactions, has only increased by two percent.

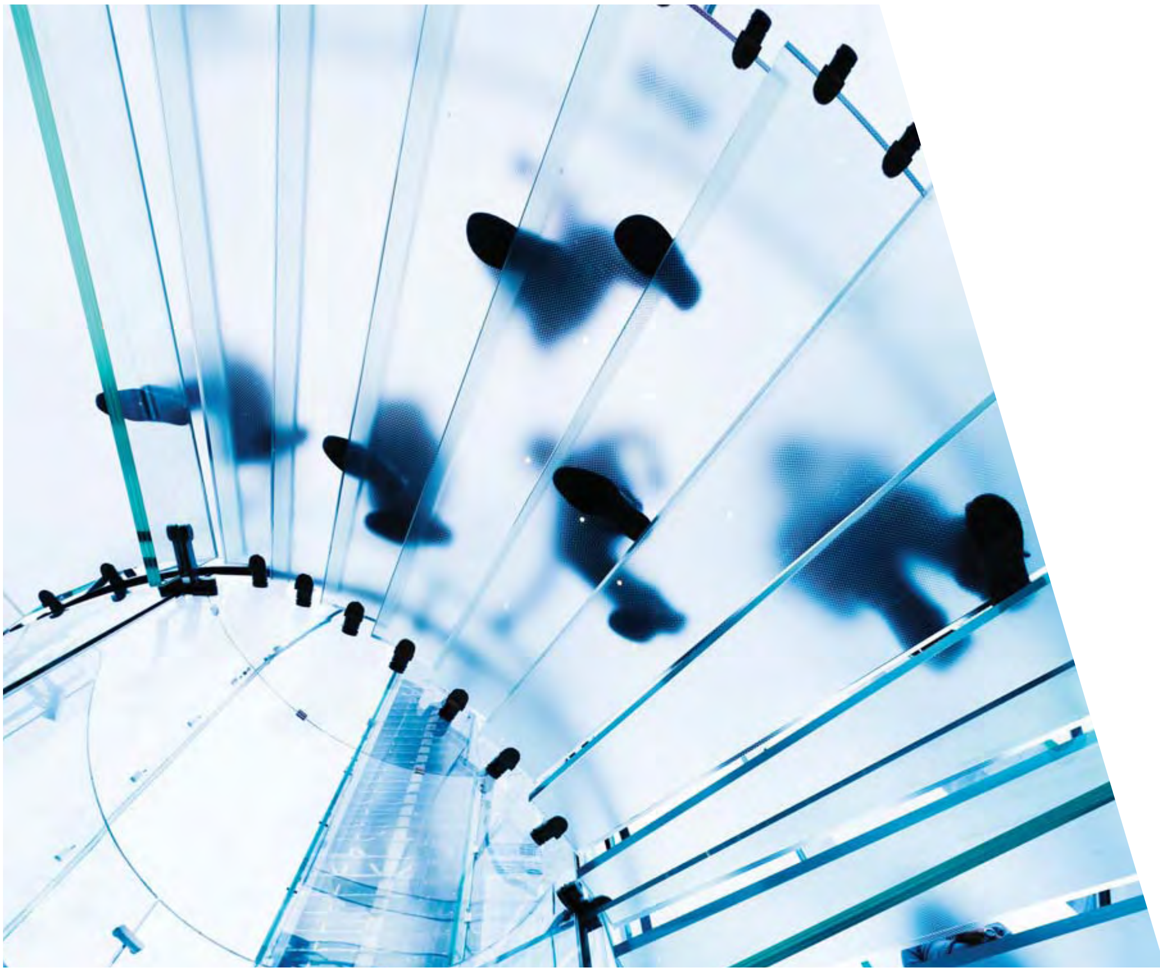
Across all regions, a customer's risk rating is primarily reviewed either periodically (74 percent of respondents) or when a client change occurs (73 percent).

Approximately half of respondents use a fixed percentage shareholding to identify beneficial owners for whom KYC is required

Of these, only 40 percent vary the fixed percentage shareholding depending upon the risk rating of the customer. In 76 percent of these cases, the percentage shareholding is lowered for higher risk customers.

In undertaking KYC for corporate customers, it is essential to understand who has ultimate control over the entity. As a result, the corporate structure must be 'unwrapped' until a relevant individual is identified. Although it may be impractical to identify every beneficial owner, regional guidelines are available which recommend the percentage shareholding an ultimate beneficial owner should hold before KYC is required.

In our firms' experience, financial institutions identify beneficial owners holding 25 percent or more of a company, in line with the EU Third Money Laundering Directive. Many institutions lower this threshold to 10 percent for high risk customers. Where no single shareholder has a holding of 25 percent or more, consideration is given to individuals' roles in order to identify those who have decision-making power or who can exert significant influence. While some financial institutions verify the identity all of these beneficial owners, others collect the names of the beneficial owners and only verify in higher risk situations.



" **A cross-linked register of company registers accessible to banks so that they can check who the beneficiaries are… would be particularly important."**

KPMG Global AML Survey respondent

Seventy-four percent of respondents identify all directors and controllers

Identification of all directors and controllers can be an onerous task, but is more prevalent within Central and South America and the Caribbean, Middle East and Africa and the Russian, Baltic and CEE regions, with more than 80 percent of respondents adopting such an approach. The additional due diligence work undertaken in these three regions may arise from adherence to a more prescriptive legislative framework, or institutions choosing to adopt a more thorough approach than required.

In our experience, institutions are increasingly identifying all directors, and verifying the identity of a sub-set of those directors. For controllers they tend to identify and verify only the relevant beneficial owners (i.e., those above a set percentage).

What do we think?

Data quality is central to the success of any screening or monitoring technology, as well as being critical to the wider AML decision-making process. The ability to obtain and maintain this data will be determined by a business's data governance arrangements; in effect, this means who owns the core data that is being relied upon, and what measures are in place to ensure that it is complete, consistent, accurate and up-to-date?

Recent sanctions compliance and KYC investigations have identified worrying gaps in the KYC data maintained by a number of financial institutions. Although many are looking to remediate files to address the deficiencies identified, fewer are examining their data governance arrangements to determine whether they are likely to have gaps in this data in the future. This is something we would strongly recommend.

Our client work tells us that, ultimately, accountability is at the heart of this issue. Identifying who is responsible for collecting and maintaining this information is not enough; financial institutions must have clarity as to those data items that are critical to the AML decision-making process (including screening and monitoring arrangements), who owns this data (as much of it is likely to come from the business not solely from compliance teams) and ensuring that controls are in place to gather and maintain this critical data. Often there is an assumption that client data is owned by the AML team and not by the front office. In KPMG firms' experience, this is a recipe for disaster.

Much of the data needed for effective ongoing monitoring is also required for wider business processes and decision-making, for instance basic identity data such as ownership and organizational structure to confirm credit exposure. As long as KYC is treated as a compliance issue, as opposed to a business issue, it is unlikely that institutions will deliver robust and sustainable controls for maintaining quality and consistent data.

As FATCA is implemented during 2013 and 2014, the ownership of the data collection process will become a focus. Any institution conducting a remediation exercise now should consider the FATCA requirements, so that they don't have to conduct additional remediation later. However, most AML teams are awaiting guidance from their tax teams before doing so, and therefore may miss this opportunity.

Any institution conducting a remediation exercise now should consider the FATCA requirements, so that they don't have to conduct additional remediation later.

Regulators are active, but banks want a more collaborative approach

Eighty-five percent of banks feel that the overall level of regulatory burden is acceptable, but most of these believe the requirements themselves need to be better focused to combat money laundering more effectively

Regulators have reviewed a number of key areas since the last survey in 2007, focusing especially on KYC (at 88 percent of respondents), AML due diligence for high risk customers (at 86 percent of respondents) and transaction monitoring (at 83 percent of respondents). However, many believe that there is a need for their approach to be better focused, in particular the North American and ASPAC banks surveyed (67 percent and 61 percent respectively).

For those who wanted changes in AML regulations and regulatory approach, we identified two distinct suggested areas for improvement from the responses given

- More guidance (14 percent)

"The regulations should provide more guidance, not just monitoring and penalties."

"The AML regulations imposed on financial institutions by governments should be about encouragement and guidance rather than about fines and penalties."

- A collaborative approach (12 percent)

"There should be a collaborative approach rather than a punitive approach; this would make a huge difference. Banks are trying to make efforts out of fear of sanctions rather than a collaborative approach."

Banks also want a more collaborative approach from the non-regulatory authorities

"I would like to see better sharing between government and financial institutions. It's a one-way direction that goes straight to the government, there's no sharing of information back from the government. I think it's a waste of energy without having key information for us."

"The government should invite the banks and involve and consult with banks regarding new laws."

"I think the best thing they could do would be to enhance their collaboration between different countries and regions."

Only half of European institutions had their correspondent banking program reviewed by regulators within the past three years

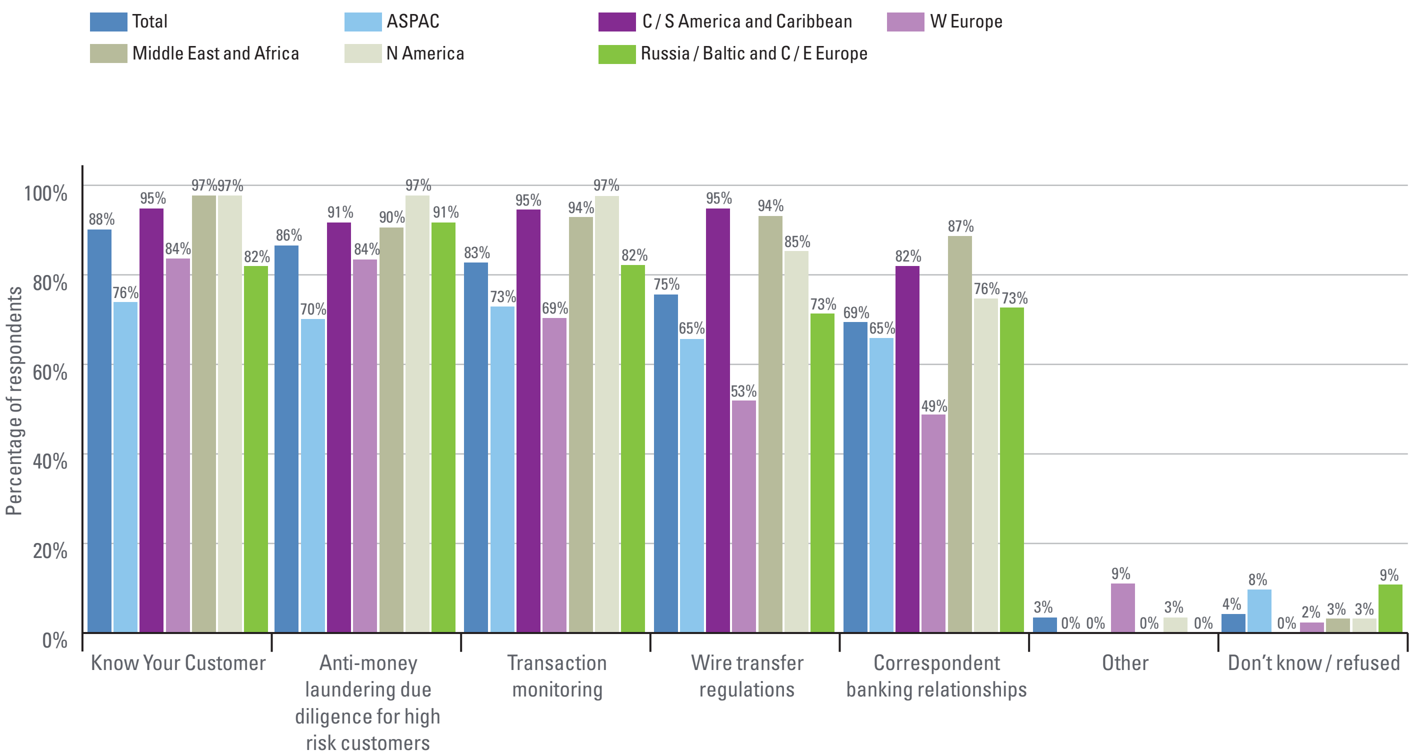
Correspondent banking appears to be a lower priority for European regulators. As a consequence, financial institutions in the region have not focused as much attention on issues surrounding this area. Conversely, regulators within Central and South America and the Caribbean and the Middle East and African regions were more proactive in this area (82 percent and 87 percent respectively).

Cover payments, and the transparency thereof, is an issue affecting all financial institutions, hence the introduction of the new MT202COV message by SWIFT. Given the lower interest by regulators in this area, it may not be surprising that European institutions lag behind the other regions in their use of the message type (as described on pages 23 and 24).

Many believe that there is a need for [regulators'] approach to be better focused.

Figure 16

Areas reviewed by regulators within the last three years



What do we think?

International regulators remain active in the areas of AML and sanctions. As already mentioned, fines can run to hundreds of millions. However, there is a clear perception that regulators and other authorities could do more to collaborate with the industry to fight financial crime. Furthermore, there is a wide disparity between the focus of regulators in the three main geographical regions:

- *In the Americas, regulatory focus continues in intensity. Examiners maintained pressure on areas they consider high risk, such as correspondent banking, and currency intensive lines of business, however they are now looking more closely at other businesses as well, including those with a primarily institutional client base. While regulators continue heavily scrutinizing transaction monitoring and sanctions compliance, they are paying increased attention to customer due diligence. As a result, KPMG firms' see many clients undertaking KYC remediation exercises that are risk-based in focus. To withstand regulatory scrutiny, financial institutions find themselves implementing programs that are a combination of rules-based and risk-based.*
- *In Europe, the Middle East and Africa, initial CDD is scrutinized more closely than transaction monitoring. The emphasis is on ensuring that banks do not take on clients that would be considered undesirable. This agenda sits uncomfortably with the desire to ensure that banking is available to all. In some cases it is simply too expensive to take on higher risk customers, and some banks have started to charge higher risk customers a premium to cover the compliance costs of dealing with them.*
- *In ASPAC, with the exception of Australia, the regulators tend to have fairly prescriptive and inflexible rules, whilst being far less active in enforcement than the other regions. The geographical spread of the region also means that there are numerous and sometimes conflicting requirements. This makes it difficult for global institutions to ensure compliance with all of their global requirements.*

Concluding remarks

In our 2007 survey, we concluded that a move towards a risk-based approach was to be welcomed, but for that to be successful it needed commitment by both the banks and their regulators. So have these stakeholders delivered on this commitment?

In terms of the banks and other financial institutions, it is clear that most have continued to commit significant resources to addressing AML risks and issues. Furthermore, despite the other pressing issues dominating senior management's attention (including at times the very survival of their businesses), AML continues to have traction at a senior level albeit somewhat reduced from the pre-crisis situation. On the face of it, the signs are that the banks have stepped up to meet their obligations.

The results of the survey and the action taken by certain regulators globally, however, suggest that the banks still have some way to go. The investment has been made, senior management has been (by and large) engaged, but something is still missing. Understandably perhaps, it is in the more challenging areas of embedding cultural change and delivering effective ongoing monitoring (and calibration) arrangements where further effort is required. Having the systems in place is not enough; the management of these risks should be suitably dynamic, with necessary skills, tools and accountabilities in place. Only this can help ensure that those attempting to exploit the world's financial institutions for the purposes of financial crime are identified and stopped at every turn.

If the banks have more to do, what about the regulators? In 2007, we identified the need for greater feedback, consultation and better communication of good practice and it seems there is still room for improvement here. Whilst there has been progress – for instance, the current consultations for more meaningful definitions of PEPs and beneficial ownership – banks still feel that more collaboration is needed. Although our respondents made it clear that they would like to see a more joined-up approach between the regulators, governments and Financial Intelligence Units (FIUs) and the banks, perhaps the greater challenge is how effective AML is delivered in the context of some of the other pressures being faced, including sanctions compliance and FATCA. A more holistic (and complementary approach) to the management of client data would be beneficial for banks in order to meet these challenges.

In summary, there continues to be commitment by all parties to make their interactions work as effectively as possible. The challenge for the next three years is to ensure that the overall objective is not lost, and that the systems and controls in place are effective in frustrating those seeking to abuse the global financial system to further their own illicit ends.

Top 10 AML tips for Risk Committees and Boards

A) Verifying that AML remains cost effective

With pressure on costs, maximizing the cost effectiveness of AML is critical. Banks should consider:

1 *Moving lower risk activities (e.g., sanctions list management, gathering KYC from public sources) to lower cost locations.*

2 *Maintaining a central repository of KYC information to prevent duplication of effort across business areas and jurisdictions.*

3 *Combining KYC collection processes with other client data requirements such as legal and credit documents.*

4 *For corporate and investment banking, conducting background checks at the lead stage to avoid long sales pursuits for clients that are subsequently rejected.*

5 *Assigning ownership of client data to ensure that it is kept up-to-date when opportunities arise, rather than requiring expensive remediation exercises.*

B) Asking the right AML questions

It is critical that Boards ask the right questions of their AML teams in order to have reassurance that the AML program is effective. The types of questions they should ask may include:

6 *What themes have arisen out of the assurance and testing program, and how are they being addressed?*

7 *What does the annual MLRO report highlight as the main risks and how are they being managed?*

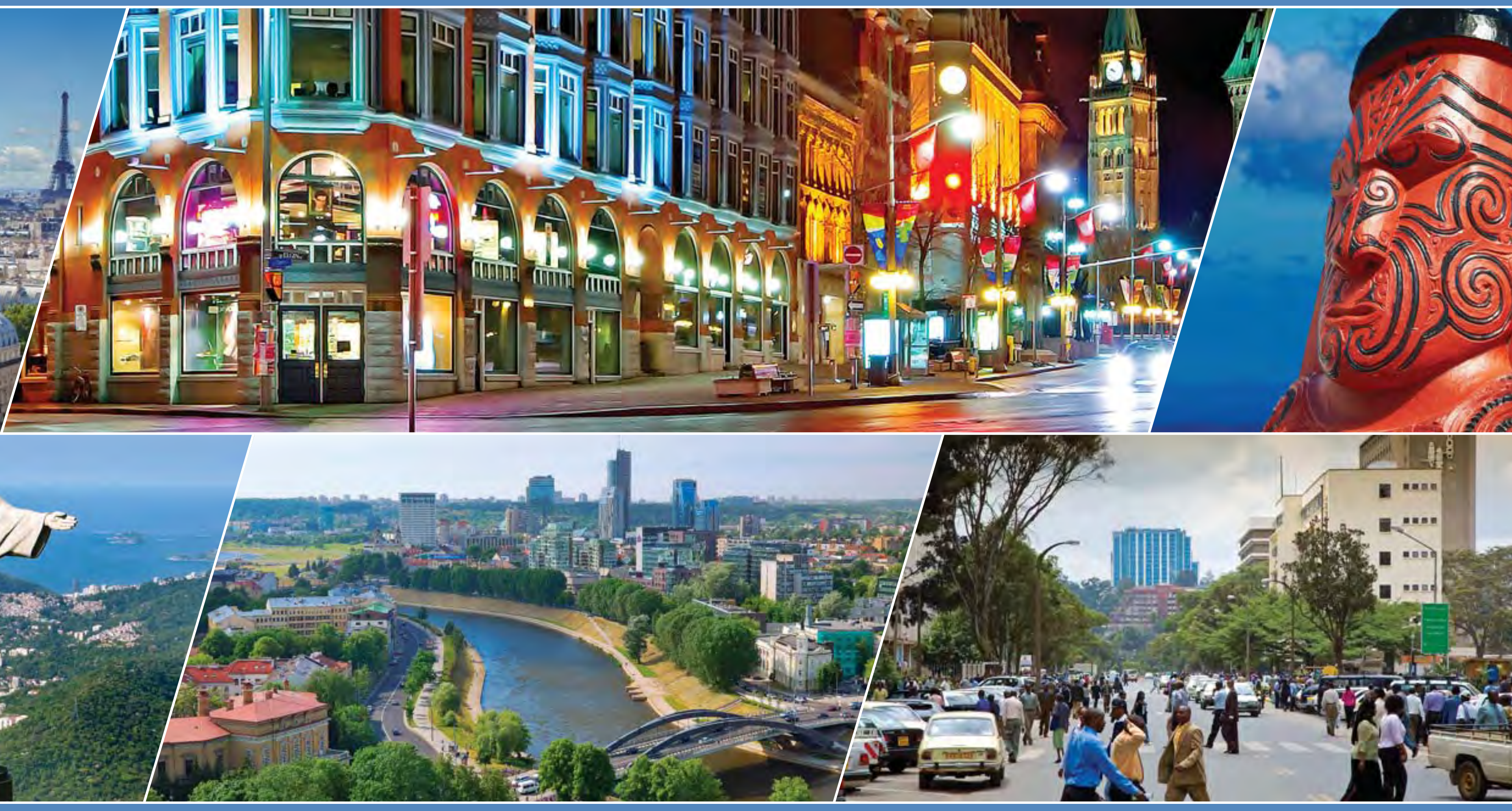
8 *What are the emerging issues that will require the AML program to adapt?*

9 *When was the AML program last tested by the Internal Audit function, and what were the results?*

10 *What activities sit outside of the core processes and systems, and how are they managed?*

Having the systems in place is not enough; the management of these risks needs to be suitably dynamic, with necessary skills, tools and accountabilities in place. Only this will ensure that those attempting to exploit the world's financial institutions for the purposes of financial crime are identified and stopped at every turn.

Regional commentaries



The regional commentaries look in more depth at the specific results for that geographical region. They also contain the opinions of our firms' local AML professionals on what the results tell us about how AML is addressed in the region, the relative strengths and weaknesses of that approach and where future attention should focus.

Western Europe

Enric Olcina
KPMG in Spain

Matthew Russell
KPMG in the UK

Steps have been taken throughout the EU in recent years to create a consistent approach to the prevention and detection of money laundering and terrorist financing. One such step was the implementation of the EU Third Money Laundering Directive to align the regulatory regime within the European Economic Area with the FATF Recommendations through the promotion of a flexible risk-based approach.

AML remains a significant risk and cost, and senior management interest is decreasing compared to other regions

The importance of AML to European senior management is falling, with only 55 percent of respondents stating that AML was a high profile issue in which the main board of directors took an active interest (down from 70 percent in 2007). This may in part be due to the implementation of the EU Third Money Laundering Directive, leading to a temporary increased focus by senior management in 2007 before returning to a level comparable to that in 2004 (60 percent). Once policy and procedural changes had been implemented, the focus of senior management on AML may have lessened.

This decrease is reflected by a reduction in the percentage of respondents who stated that AML was discussed formally by the board of directors on a quarterly basis (35 percent, down from 52 percent in 2007). Yet, for reasons set out at the start of this report, senior management would be strongly recommended to take another look at this.

Within Europe, 82 percent of respondents stated that the cost of AML compliance had increased over the last three years, with enhanced transaction monitoring being cited as the main reason. Seventy-one percent of respondents were of the view that the cost of AML compliance would continue to increase in the future.

Although AML costs have continued to rise, only 18 percent of respondents had considered off-shoring or outsourcing some of their AML functions, with 75 percent having never considered this as an option.

The percentage of European financial institutions that formally test or monitor their AML systems and controls has risen from 70 percent in 2007 to 76 percent. This is low, though, compared to the average across all regions (84 percent).

Politically Exposed Persons: EU Third Money Laundering Directive increases standards

In our latest research, 96 percent of European respondents said they considered whether a customer was a PEP for the purposes of conducting due diligence at the account opening stage. This was an increase from 75 percent in 2007. Furthermore, 94 percent had specific procedures in place for identifying and monitoring PEPs on an ongoing basis (up from 65 percent in 2007). In the overwhelming majority (84 percent) of cases, this involved either the use of commercial lists, or a combined approach of commercial lists with in-house additions. These increases are in line with expectations following the implementation of the EU Third Money Laundering Directive, which required financial institutions to identify PEPs at the account opening stage and to have in place appropriate measures to deal with such individuals.

The importance of AML to European senior management is falling.

Sanctions compliance remains a challenge

The screening of individuals against appropriate sanction lists at both the on-boarding stage and on an ongoing basis, together with the screening of payments to / from these individuals, is a key step in the prevention of terrorist financing. Sixty-one percent of European respondents stated that they found the screening of customers to be challenging or very challenging, while 73 percent said the same about the handling of filtered hits.

In recent years Europe has felt the extra-territorial reach of U.S. legislation, and in particular OFAC, resulting in a number of high profile fines.

In spite of this, one-third of European financial institutions do not screen incoming SWIFT messages for incomplete originator information. Forty-five percent of those that do, stop a transaction when details of the originating party are missing. Of those European financial institutions that do not stop such transactions, 67 percent had no plans to change this practice in the future.

Only a quarter of European financial institutions stated that they always use the MT202COV, with 10 percent using it most of the time when undertaking cross-border transactions. As a result, the majority of European financial institutions do not provide details of the originating and beneficiary parties to their correspondent banks, preventing the latter from fulfilling their sanction screening obligations.

Satisfaction with transaction monitoring systems has decreased despite evidence of increased effectiveness

Transaction monitoring continues to be the largest AML compliance cost driver for European financial institutions, although there has been a slight decrease since 2007 in the level of satisfaction with their monitoring systems.

That said, 43 percent of European respondents said there has been an increase in the number of SARs made to law enforcement agencies compared to 2007. This indicates that despite lower satisfaction levels, transaction monitoring systems are becoming more effective.

Risk-based approach: the way forward

The EU Third Money Laundering Directive introduced a risk-based approach to undertaking KYC. As a result, the number of respondents adopting such an approach rose from 83 percent in 2007 to 92 percent.

An advantage of adopting a risk-based approach is it allows financial institutions to implement an AML program that reflects their customer base and global reach. As such, no two AML programs will necessarily be the same. For example, when considering KYC for corporate customers, 57 percent of European respondents stated that the number of directors and controllers identified or verified was dependent on the risk category of the customer. Forty-eight percent of respondents identified all directors and controllers. Of those directors and controllers that are identified, their identity is verified by 55 percent of respondents.

In our member firms' experience, financial institutions have historically identified two directors and controllers. However, in recent years, and particularly following recent regulatory enforcement cases, many have moved to identifying all directors and controllers in order to screen for sanctions, only verifying one or two in higher risk situations.

Almost all (96 percent) European financial institutions have a remediation program in place to update KYC information for their customers. This represents an increase from 73 percent in 2007. It is possible that this increase is, in part, a consequence of the investigations initiated by law enforcement and other regulatory agencies in relation to alleged weaknesses in sanctions compliance. Quite often, these investigations have drawn attention to significant gaps in the KYC information maintained by financial institutions. In these circumstances a remediation program is required to satisfy senior management, as well as the authorities.

Outlook

Since the 2007 Survey, the focus on AML and sanctions compliance controls by regulatory bodies across Europe has continued to intensify. An EU Fourth Money Laundering Directive is currently being prepared and it is clear that there is a desire to make the regulatory environment work. This is likely to be expressed in terms of further clarification for some of the key concepts underpinning the regime (such as defining PEPs or beneficial ownership), as well as reiterating that systems and controls need to retain a degree of flexibility to combat organised criminals, money launderers and terrorists effectively.

Financial institutions will also need to assess the AML and sanctions compliance risks presented by emerging technologies. The internet continues to evolve as a key distribution channel for both new entrants and established constituents of the financial services community, with transactions and relationships being initiated and maintained with no or minimal customer contact. Institutions also have to understand and manage the risks presented by other technological developments, such as mobile banking, including the involvement of other third parties in the banking value chain (such as telecommunications companies). Technology is also likely to present certain opportunities – a number of software vendors, for example, are positioning themselves in response to developments in cloud computing.

In this climate, it does not pay to stand still. Whether it is the continued attention of the regulator, or changes to the environment in which they operate, AML teams need to be on the front foot in order to be successful.

North America

Teresa Pesce
KPMG in the US

Robert Skrzypczak
KPMG in the US

Regulatory expectations have been raised following the recent financial crisis, placing significant and new requirements on financial institutions. From Dodd-Frank to an increased focus on the Foreign Corrupt Practices Act to the major enforcement actions brought by the U.S. against international banks due to AML, sanctions and tax compliance transgressions, financial institutions are under greater pressure to ensure that their systems and controls are capable of dealing with an ever-increasing regulatory burden. There is also a growing sense that financial institutions must be able to anticipate changing regulatory expectations and standards, quickly adapting their compliance programs to meet these new expectations.

AML remains a significant risk and cost… and is reflected in the interest shown by senior management

Fifty-eight percent of North American respondents considered AML to be a high profile issue in which the main board of directors took an active interest. Whilst this is down from 2007 (63 percent) the number of financial institutions where AML was formally discussed at least quarterly by the board of directors has risen from 40 percent in 2007 to 61 percent. This increase is due to those financial institutions that in 2007 discussed AML annually now discussing AML matters on a quarterly basis.

Of all of the regions surveyed, North America had the smallest percentage of financial institutions (64 percent) reporting that AML investment had increased during the previous three years. A possible explanation may be that some financial institutions reduced, or kept static, their spending on AML as they focused on controlling costs in order to weather the financial crisis. Of those financial institutions that reported higher AML expenditure, almost half reported an increase of at least 51 percent. 'Investment in enhanced transaction monitoring systems' was cited as the primary reason for the increased spending.

Given the focus by financial institutions on controlling costs, it is surprising that 97 percent of North American respondents reported they had neither off-shored nor outsourced AML functions to lower cost locations. Most of these financial institutions said they had not even considered doing so. This is likely because there is a perception that US regulators will not support offshoring outside of American shores.

Of all of the regions surveyed, North America had the smallest percentage of financial institutions reporting that AML investment had increased during the previous three years.

Going forward, three quarters of North American respondents expect AML expenditure to continue to grow, though the pace of growth is expected to slow. Interestingly, respondents made a similar projection in the 2007 survey, which proved to be optimistic for many.

The U.S.A. PATRIOT Act identifies four primary AML requirements that must be met by covered institutions, one of which is the requirement that financial institutions have an independent system for testing their AML systems and controls. Canada's Office of Superintendent of Financial Institutions has mandated that Canadian financial institutions test their AML programs annually. As a result, 92 percent of North American respondents stated they have a formal monitoring system in place, but this means that eight percent do not engage in the annual testing of their AML processes.

Politically Exposed Persons: the scrutiny intensifies

The identification of foreign PEPs remains a key requirement under the U.S.A. PATRIOT Act. While the identification and risk mitigation processes associated with PEPs remains a high priority, only 86 percent of North American financial institutions reported they had specific procedures in place to identify and monitor PEPs.

A possible explanation for this is that, as domestic PEPs are not captured by U.S. PEP regulations, U.S. financial institutions with a purely domestic client base may not have developed processes to identify and review PEPs, whether foreign or domestic. Going forward, it will be interesting to see if regulatory authorities change their position on excluding domestic PEPs from heightened identification and review requirements, especially as international AML bodies consider recommending that domestic PEPs be treated in a manner similar to foreign PEPs.

Sanctions compliance remains a challenge
OFAC administers various country and list-based economic sanctions programs promulgated by the United States. KPMG firms' have continued to witness significant enforcement actions targeting OFAC violations involving large global financial institutions. Certain of the enforcement actions have been brought as deferred prosecution agreements with significant fines, the requirement to conduct substantial 'look backs' and future commitments, including implementing strengthened controls and enhanced training requirements. In this context, the majority of respondents reported that they found aspects of sanctions compliance to be 'challenging' or 'very challenging' (particularly the handling of filter hits (72 percent); client screening (69 percent); and trade finance (64 percent)).

The screening of customers and transactions against these lists is a resource-intensive exercise. Unlike AML transaction monitoring, where activity is monitored, alerts investigated and reports made, if necessary, after the fact, sanctions screening is done in real time. Transactions stopped by filters must be investigated immediately and rejected or blocked if any true 'hits' are identified, with reporting required in short order. Knowing one's customer is critical in the area of sanctions screening. For example, institutions must not only screen named account-holders, but should also screen material beneficial wners and signatories.

In response to problematic activity criticized in a number of OFAC enforcement actions brought over recent years, there have been substantial changes in the requirements associated with sanctions compliance. Most immediately, a new wire transfer message type (MT202COV) was developed in order to increase transparency in the use of certain types of SWIFT messages to facilitate transaction screening by intermediary banks in the payment chain. In this regard, only slightly more than half of North American respondents reported using the new message type.

Another area of regulatory focus has been on ensuring that financial institutions populate SWIFT messages with complete originator information and that receiving institutions survey incoming messages in order to identify SWIFT messages that are missing such information. Our survey reflected that only 60 percent of North American financial institutions screen SWIFT messages for incomplete

Only slightly more than half of North American respondents reported using the new [MT202COV] message type.

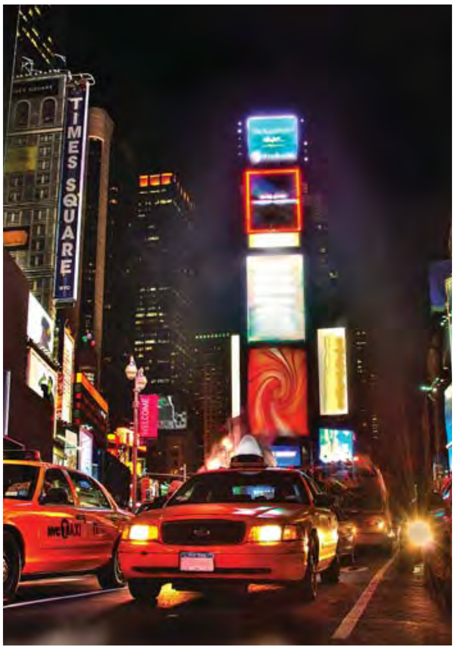
originator information. Of that 60 percent, only 68 percent reported that they were stopping messages with incomplete originator information. Of particular surprise is that 11 percent of North American respondents reported that they did not populate originator information in SWIFT messages; this is in apparent contravention of the Financial Crimes Enforcement Network's (FinCEN's) longstanding Travel Rule and FATF VII. It will be interesting to see if deficiencies in these areas become the subject of future regulatory examination findings or enforcement action.

Financial institutions split over the effectiveness of transaction monitoring

As was the case in the 2007 survey, the majority of North American respondents indicated that 'increased transaction monitoring activity' was the key factor in the rising cost of AML.

Possibly as a consequence of their higher investment in IT, 47 percent of internationally active North American financial institutions said they were able to monitor a customer's transaction and account status across multiple countries, compared to 32 percent globally. In an interesting split, 14 percent of respondents reported that their transaction monitoring system was 'very satisfactory' while 20 percent of respondents reported that their transaction monitoring system was 'very unsatisfactory'. Approximately 40 percent of respondents reported that their transaction monitoring system was 'satisfactory.'

In line with our experience from the 2004 and 2007 surveys, North American financial institutions continued to report the filing of an increased number of SARs, with 81 percent reporting either a 'substantial increase' or 'some increase'. However, one pattern that emerged from the survey is that the number of financial institutions that reported a 'substantial increase' in the number of SARs filed fell from 63 percent in 2007 to 28 percent in the current survey, so the pace of increase appears to be slowing.



Eighty-three percent of North American financial institutions reported having a process to remedy gaps in KYC information maintained for existing customers.

Remediation of gaps in KYC not undertaken by all

The survey showed no change in the percentage (83 percent) of financial institutions applying a risk-based approach to determining KYC requirements associated with the acceptance of new clients. This compares to 91 percent for the global population. The difference may be attributable to the fact that, historically, U.S. broker-dealers have taken a more rules-based approach to verifying the identity of new clients. In coming years, it will be interesting to see if this statistic moves in the direction of the global average.

Eighty-three percent of North American financial institutions reported having a process to remedy gaps in KYC information maintained for existing customers, up by three percent from the 2007 survey. A variety of approaches are utilized, including gathering KYC information when the customer transacts new business or opens a new account (42 percent), taking a risk-based approach (28 percent) or reviewing the entire customer base on a regular basis (14 percent). Seventeen percent of North American financial institutions reported that they have no program in place to refresh KYC information associated with existing clients.

One reason for the lower percentage of North American respondents that have processes in place to update KYC information, when compared to the global average of 93 percent, may be due to U.S. financial institutions placing great emphasis on, and investing heavily in, AML transaction monitoring systems as opposed to refreshing or remediating gaps in KYC information. Another contributing factor may be that the primary U.S. AML regulations do not mandate that financial institutions take a risk-based approach to on-boarding most new client types nor require that most types of KYC information be refreshed on a periodic basis, although banking examiners certainly look for this when conducting AML examinations. As a result many U.S. financial institutions do engage in such periodic reviews, in response to examination guidance published by the U.S. banking regulatory agencies, examination findings, or as best practice.

Outlook

Significant legal and regulatory pressure in the region over the last few years has created a more challenging AML landscape. As part of our 2007 survey, we questioned what future direction U.S. AML regulation and enforcement would take (principles versus rules). With increasingly larger fines and additional new regulation (such as the Unlawful Internet Gambling Enforcement Act) it would appear that the U.S. continues to take a more 'hard-lined' approach to AML compliance compared to the rest of the world.

In the near term, financial institutions are facing significant new regulations, which will require considerable attention including the FATCA, the proposed Cross-Border Electronic Transmittal of Funds Reporting Rule and the possible expansion of AML program requirements to hedge funds and private equity funds.

While continuing strictly to apply rules, regulatory guidance and examination experience indicates that U.S. regulatory authorities do and will continue to overlie a rules based structure with a risk-based approach. The Federal Financial Institutions Examination Council's (FFIEC) BSA / AML Examination Manual mandates that examiners look for, and if necessary, conduct risk assessments of the institutions they examine, and test based on risk. Examination reports requiring institutions to update programs based on risk, particularly in the area of KYC, bear this out. Additionally, in 2010, U.S. regulatory authorities issued Joint Guidance on Obtaining Beneficial Ownership Information.

While there has been some debate about the statutory authority supporting the substance of the guidance, the guidance recommends that financial institutions should take a risk-based approach in determining when they should obtain beneficial ownership information regarding clients.

Whether U.S. authorities are ready to move towards a more flexible approach to AML remains to be seen. If history is a guide, however, it is likely that there will be no substantial or practical easing of the regulatory burdens faced by U.S. financial institutions and we should expect to see a steady stream of new regulations and enforcement actions.

Asia Pacific

Gary Gill
KPMG in Australia

Jeremy Allan
KPMG in Australia

ASPAC is a diverse region with many different jurisdictions therefore it is, to some extent, difficult to make generalizations or draw conclusions, as one jurisdiction may be very different from another. For example, some ASPAC jurisdictions have scored very highly in FATF reviews, while others have not. Nothing said here should be taken as a comment on a particular jurisdiction or regulator.

The lower public profile of AML in ASPAC may be linked to the fact that the level of public regulatory enforcement action has been lower than in other regions of the world.

ASPAC firms look first outside of ASPAC for AML guidance

Across ASPAC, the last three years have seen the introduction of a number of new pieces of AML legislation, which to date have not been accompanied by significant enforcement action by local regulators. As such, global financial institutions operating in the region continue to invest more in AML than their local counterparts, driven by expectations of regulators from more mature AML and sanctions regimes.

Global financial institutions typically set local AML policies within ASPAC by first referring to the global AML policy. Local ASPAC institutions, however, normally refer first to their home country regulations in order to develop policies and procedures. The result tends to be that the global institutions operating within ASPAC have AML policies and procedures with wider coverage than those developed by their competitor banks within the same markets.

Senior management consider AML to be a lower profile issue compared to other regions

The survey suggests that AML is viewed as less of a high profile issue within ASPAC financial institutions. Across the ASPAC financial institutions surveyed, 50 percent stated that AML was either a moderate or low profile issue in which the board of directors takes some or little interest. This was 12 percent lower than the global average. Also, AML is discussed at board level by ASPAC financial institutions at least annually by only 27 percent, markedly less frequently than the global average.

The lower public profile of AML in ASPAC may be linked to the fact that the level of public regulatory enforcement action in ASPAC has been lower than in other regions of the world.

In those ASPAC jurisdictions where the regulator has taken public enforcement action in recent years, the penalties applied have been relatively small by European and U.S. standards. For example, while the regulator in China has fined a relatively large number of financial institutions for suspicious matter reporting deficiencies, the size of the fines imposed has been less than USD100,000 in each instance. Equally in Australia the public enforcement action taken so far by the regulator has been limited to the relatively small subsidiaries of two international banks, and some money service bureaux.

It is worth noting, however, that while there may have been less public enforcement action by ASPAC regulators, anecdotal evidence would suggest that banks have been subject to scrutiny which has not been made public.

Anecdotal evidence would also suggest that the frequency of discussion of AML at board level in ASPAC might change in the short-to-medium term due to the advent of FATCA. With the expected increase in funding to comply with FATCA likely to be significant enough to require board approval, institutions are seeking to identify ways in which current AML systems, processes and technology can be leveraged to minimize the increased funding required. In this context, board consideration of AML and FATCA together is recognized as being key.

Linked to AML's board level profile, survey respondents within ASPAC also suggested that investment in AML over the last three years had increased by 10 to 20 percent, compared to an increase globally of 20 to 50 percent for the majority of institutions. The outlook for investment in AML in ASPAC was similar. Ninety-five percent of financial institutions surveyed expected investment in AML to increase over the next three years, though 43 percent (the largest category) expected the increase to be only 10 to 20 percent.

The three main drivers of the higher cost of compliance in ASPAC over the last three years were increased internal reporting requirements, increased external reporting requirements and enhanced transaction monitoring. This is borne out by evidence from Chinese institutions where regulatory enforcement action has centred on deficiencies identified in suspicious matter reporting, which in turn has led to more focus being applied to this area.

Politically Exposed Persons: the scrutiny intensifies

The survey shows some interesting results in respect of the identification and monitoring of PEPs within ASPAC.

Survey participants in ASPAC stated that only 73 percent have specific procedures in place for identifying and monitoring PEPs on an ongoing basis, against 88 percent across the global survey. The survey shows that progress is being made by the ASPAC survey participants in this area. Since the 2007 survey, the number of institutions with specific PEP identification and monitoring procedures has risen by 31 percent, which compares well with the increase noted in European institutions. There is, however, further to go.

The rationale for ASPAC lagging behind other regions in identifying and monitoring PEPs is complex. Given the nature of some of the governments in the region, identifying domestic PEPs may prove challenging. There are further complicating factors, such as local regulators in Hong Kong, China, Singapore and Japan releasing their own lists of undesirables or anti-social organizations with whom institutions should refrain from transacting.

Anecdotal evidence would suggest that local institutions within these countries devote more time and resource to identifying those whom their local regulators prescribe, as opposed to PEPs, which can be more subjective. It is also simpler for institutions to identify and monitor such undesirables as the lists are compiled and released by local regulators, and are only available from them, as opposed to PEP lists which are commercially available but more open to debate and interpretation.

Anecdotal evidence would suggest that the frequency of discussion of AML at board level in ASPAC might change in the short-to-medium term due to the advent of FATCA.

Sanctions compliance remains a challenge

The area of sanctions compliance that ASPAC institutions reported as being most challenging was that of trade finance, with 32 percent of respondents describing it as very challenging, which was 10 percentage points higher than the global average. With a large proportion of global trade finance routed through ports in ASPAC, this is an area of concern, especially given the problems associated with consistently translating names correctly from, for example, Mandarin to English for screening purposes.

Lists are released by regulators such as the Hong Kong Monetary Authority (HKMA), the Japanese Ministry of Finance, the Australian Department of Foreign Affairs and Trade (DFAT) and the Monetary Authority of Singapore (MAS). As well as the UN Sanctions, financial institutions operating in ASPAC are mindful of the OFAC Sanctions regime, which has taken some enforcement action in the region.

Enforcement action taken by U.S. regulators in other regions has led global institutions to re-examine their existing sanctions compliance programs. The effect of this has been that such institutions now have mature global sanctions solutions, which may be in advance of the local expectations in some ASPAC jurisdictions.

Outlook

We stated in our 2007 survey that AML was clearly moving up the corporate agenda for financial institutions in the ASPAC region and that global banks would have a very important role to play in helping shape the AML environment within the region based on their experience in other parts of the world.

The results from our latest survey suggest that while AML is becoming more important to organizations within ASPAC, and that progress is being made, there is still more to do. Interestingly, 13 percent of ASPAC respondents in this survey called for stricter enforcement of the AML regulations, against an overall average of seven percent. This may be due to banks wishing to gain a greater understanding of how the regulations should be implemented, which may become an area of greater focus over the next three years.

Central and South America and the Caribbean

Teresa Pesce
KPMG in the US

Robert Skrzypczak
KPMG in the US

Banks in this region have stepped up their game to meet growing regulatory challenges. As there is increased focus from Boards of Directors, there has been an almost universal increase in investment in AML programs, in particular around transaction monitoring. With corruption a concern in the region, banks are rising to the challenge with risk-based KYC programs, and a focus on PEPs. Based on international focus on the region, we can expect to see Banks stepping up to meet even greater challenges in the future.

AML and sanctions compliance remains a priority in the region, with 96 percent of respondents saying AML maintains a high profile with the board of directors.

AML remains a significant risk and cost… and senior management are taking an active interest

This survey shows AML and sanctions compliance remains a priority among financial institutions in the region, with 96 percent of respondents saying AML maintains a high profile with the board of directors, which considers AML issues on at least a quarterly basis.

A greater proportion of financial institutions (91 percent) in the Central and South America and Caribbean region than in any other region reported that AML spending had increased during the previous three years. Of these, approximately 70 percent reported AML spending increases of 20 percent or more. Financial institutions in the region attributed the rise in costs to increased expenditure on transaction monitoring (also cited in the 2007 survey) as well as training. In an emerging trend, 'anti bribery and corruption activities' had a strong (38 percent) or very strong (33 percent) impact on AML spending. This may be in response to the extra-territorial reach of, and heightened regulatory expectation associated with, the UK Bribery Act 2010 and the FCPA.

In line with the other regions surveyed, few financial institutions have off-shored or outsourced AML functions. This may be because many countries in the region have strong privacy laws, making it difficult to transmit client data off-shore.

Looking ahead, 87 percent of financial institutions surveyed stated that they expect AML spending to continue increasing, with more than half predicting expenditure increases of between 10 percent and 20 percent over the next three years.

Politically Exposed Persons: the scrutiny intensifies

Central, South America and the Caribbean was the only region in which every financial institution reported that they had a procedure in place to identify and monitor PEP relationships. Respondents reported using a variety of methods to identify PEPs, including utilizing commercial lists, internally generated lists or a combination of the two. The region's strong approach to identifying PEPs is likely dictated by notable reported cases of corruption in recent years and the fact that many countries require financial institutions to have processes to identify and mitigate the risks associated with both foreign and domestic PEPs.

With the economic ties between countries in the region and the U.S., it is not surprising that respondents consider sanctions compliance to continue to be 'very challenging' or 'challenging'.

Sanctions compliance remains a challenge

Sanctions compliance continues to present challenges, particularly in light of the increasing use of economic sanctions by governmental and supranational bodies such as OFAC, the EU and the UN, as well as aggressive regulatory enforcement actions initiated by the U.S. against international financial institutions for directly or indirectly facilitating violations of sanctions laws. In this regard, with the economic ties between countries in the region and the U.S., it is not surprising that respondents consider sanctions compliance to continue to be 'very challenging' (35 percent) or 'challenging' (52 percent), the highest combined total of any of the regions surveyed. In particular, respondents cited client screening, the maintenance of sanctions lists and trade finance as presenting particular challenges.

It is notable that the region reported among the highest rates of compliance with the principles set forth in the FATF VII. Specifically, 91 percent of financial institutions claim to include originator information within SWIFT messages. In addition, 83 percent said they screen incoming SWIFT messages for incomplete originator information. All of the financial institutions that do screen for incomplete originator information report said they stop SWIFT messages when they detect incomplete information.

There is satisfaction with the effectiveness of transaction monitoring

Reporting the highest satisfaction rates of any of the regions, financial institutions in the Central, South America and Caribbean region stated that their transaction monitoring systems were 'satisfactory' (52 percent) or 'very satisfactory' (26 percent). Financial institutions in the region also claimed a relatively high degree of functionality for their transaction monitoring systems, with 78 percent of respondents reporting that they could track a single customer across business units and 57 percent that they could monitor a single customer across multiple jurisdictions. In line with our experience from the 2004 and 2007 surveys, financial institutions in this region continue to report the highest number of SAR filings.

In a sign of the growing maturity of AML programs in the region, every financial institution surveyed said they had processes in place to test and monitor the effectiveness of their AML systems.

Perhaps surprisingly, 61 percent stated that their AML policies and procedures were developed and implemented at a regional/local level - by far the highest level reported by any region. Moreover, 30 percent said they have a global AML policy but detailed procedures are set at a regional/local level. These statistics may be a reflection of the fact that many countries in the region, such as Brazil and Mexico, have imposed specific AML requirements that can only be addressed through local policies and procedures. Of particular note is that a significant minority of financial institutions in the region (17 percent) view the burden of legislation to be excessively onerous and not effective. The most cited request for improvement was for more guidance to be provided by regulatory authorities.

Risk-based approach adopted to KYC

As in the 2007 survey, the overwhelming majority of respondents employ a risk-based approach to account-opening, using a broad range of factors to assign a risk-rating to the client, including country risk, the nature of the client's business, the products and services requested by the client, the volume and / or value of the client's anticipated business and whether the client is a PEP. In addition, financial institutions in the region reported using a three-tiered client risk-rating system (high, medium and low) which, in turn, drives the frequency with which KYC information associated with existing customers is reviewed.

Outlook

It is our expectation that the future will present further challenges in AML and sanctions compliance regionally. In particular, we anticipate the seven countries in the region – Antigua and Barbuda, Ecuador, Honduras, Paraguay, Venezuela, Bolivia and Trinidad and Tobago – that were recently cited by FATF as having strategic AML or counter-terrorist financing deficiencies will take steps to address these issues. We would also expect to see the U.S. and perhaps other jurisdictions continue to bring aggressive enforcement actions involving AML and sanctions compliance. Further, new regulations such as FATCA may require financial institutions to create additional compliance and operational infrastructures in order to comply with the new regulations.

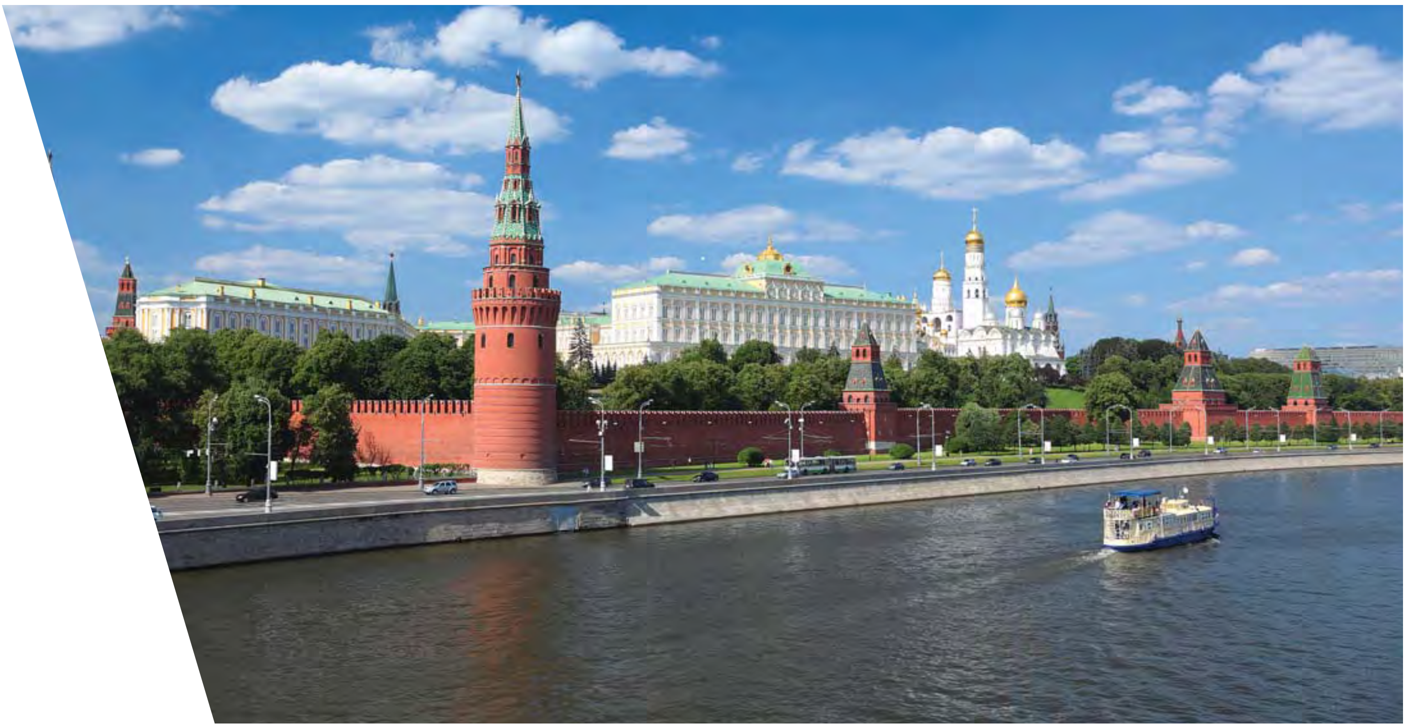
We would expect to see the U.S. and perhaps other jurisdictions continue to bring aggressive enforcement actions involving AML and sanctions compliance.

Russia, the Baltic and Central and Eastern Europe

Alex Sokolov
KPMG in Russia

Michael Peer
KPMG in the Czech Republic

The AML environment in Russia continues to be highly formal, with an emphasis on strict adherence to rules. There remain, however, a number of grey areas within the AML requirements in the region, which have led to ongoing demands for the regulator to provide clarity. This is especially the case in areas where AML deficiencies have resulted in the revocation of banking licenses.



AML remains a high profile issue for senior management

Financial institutions within the region regularly discuss AML issues at board level, with almost three quarters (74 percent) of respondents saying it is discussed either monthly or quarterly. This regularity is reflected in the fact that 60 percent of respondents in the region said AML was a high profile issue in which the main board of directors take an active interest.

As predicted in our 2007 survey, AML expenditure in the region has risen by 50 percent. Over the next three years, financial institutions expect on average a further 50 percent rise in AML costs. This is the highest expected rate across all regions.

Although financial institutions in the region previously had a lower AML expenditure base, investment is now being made into more sophisticated levels of AML. Almost half of financial institutions surveyed expect their AML costs over the next three years to be up to USD1 million, 24 percent expect between USD1 million and USD5 million, and 16 percent expect costs to be greater still.

Although financial institutions in the region previously had a lower AML expenditure base, investment is now being made into more sophisticated levels of AML.

Politically Exposed Persons: the scrutiny intensifies

Current legislation and regulation in the Russian, Baltic and CEE region requires financial institutions to identify PEPs and to have measures in place to deal with them. These amendments are in response to the recommendations of FATF and the Wolfsberg Group. It should be noted, however, that the legislation concerns the targeting of non-domestic PEPs only. International financial institutions that operate within the region consider Russian PEPs to be non-domestic from the headquarters' perspective; a similar approach is applied by the large local financial institutions that operate internationally. As a result, an expanded definition of a PEP is, in fact, applied by financial institutions.

Despite the absence of regulatory or legal requirements to identify PEPs in the past, 83 percent (69 percent in 2007) of financial institutions in the region claimed to do so. This may be driven by a wish to improve their reputational standing internationally and to enable correspondent banking relationships to be maintained with financial institutions operating in regions such as North America and Europe. Most of the respondents use combined (both in-house and commercial PEP lists) means of PEP identification. The remaining 30 percent use only commercial lists.

Sanctions compliance remains a challenge

The local 'negative list', supplemented by part of the UN sanction list, was introduced in Russia in 2003 and is regularly updated. Those financial institutions that have correspondent banking relationships with U.S. institutions also comply with the OFAC sanction lists, while those financial institutions with a European nexus also use EU sanctions lists. As local legislation does not enforce Specially Designated Nationals (SDN) and EU lists, financial institutions in the region can face a conflict in terms of which of the matches generated are reportable. This may explain why respondents see almost no challenge in the technical aspects (maintenance of lists, automatic screening) of the sanctions regime, yet the legal impact (account blocking, trade finance, handling of filter hits) gives rise to difficulties. Overall, client sanctions screening is considered challenging, or very challenging, for 67 percent of respondents. A further challenge in the region is an apparent lack of well-trained staff.

Respondents are satisfied with the effectiveness of their transaction monitoring

Enhanced transaction monitoring is the largest AML compliance cost driver for financial institutions within the Russian, Baltic and CEE region. Most respondents report that they employ a full range of monitoring techniques to some degree. Respondents also reported the wide application of sophisticated IT systems to assist in the automation of transaction monitoring. The systems currently used by financial institutions are usually vendors' products tailored to the profile of the institution.

Historically, when AML laws were introduced, vendors lacked the time or skill to develop systems quickly enough and of an acceptable quality level. As a result, financial institutions developed in-house solutions. Respondents rated their transaction monitoring systems as satisfactory, with most of them able to monitor a single customer's transaction across different business units.

In contrast to most other regions, there has been no significant increase in the number of SARs reported by financial institutions within Russia, Baltic and CEE. Only 19 percent of respondents reported a 'substantial' increase in SARs, which is half the global average (39 percent). This is likely to reflect the legislative requirement to report on a pre-defined set of transactions for so-called 'compulsory reporting'. While 42 percent of respondents said there had been a rise in the number of SARs filed, this may be due to the natural growth of the banking industry.

Testing of AML systems appears very high

AML compliance functions at financial institutions in the region tend to be smaller than those in the other regions. However, staff within these functions are well trained and experienced, reflecting the need to have local knowledge in an environment where AML requirements are not always clear in practice and information is not as readily available as in some other jurisdictions. There are ongoing and widespread efforts by financial institutions in the region to recruit staff with relevant AML experience.

Of the financial institutions surveyed in this region, 76 percent stated that they had a formal program in place to test the effectiveness of their AML systems and controls (down from 100 percent in 2007). Whilst local regulation doesn't require such systems, some financial institutions in the region are introducing them, however, in our experience 76 percent appears to be high.

All respondents said internal audit was involved in the monitoring and testing of AML systems and controls. The involvement of the compliance function in monitoring and testing AML has risen from 43 percent in 2007 to 75 percent.

Many financial institutions maintain a separate AML function, which is required under Community Based regulation (CBR) regulations to be independent. Indeed, some financial institutions have started to add a separate compliance function, giving rise to a greater role of compliance in testing and monitoring.

In addition to internal audit and compliance, operations (63 percent), external audit (88 percent), and financial crime / fraud prevention (44 percent) contribute in the monitoring and testing of AML systems and controls.

Many financial institutions in the region employ security professionals to assist them in identifying customers, finding out about their background and / or following up potentially suspicious transactions.

Remediation of KYC data undertaken by the majority of institutions

Ninety-one percent of respondents within the region stated that they apply stricter KYC requirements depending upon the money laundering risk assessment posed by the customer.

At the account-opening stage, financial institutions employ a risk-based approach, with all respondents saying the nature of the customer's business and whether the customer was a PEP were the two most important factors in assessing AML risk.
The results are driven by the CBR regulatory requirement to assign a risk level to each customer, with specific rules on how this should be done (including the nature of the customer's business, among other factors). Many financial institutions in the region employ security professionals to assist them in identifying customers, finding out about their background and / or following up potentially suspicious transactions.

Ninety-two percent of banks in the region also reported that they have a remediation program in place to fill in any gaps in the KYC information they hold on existing customers (the highest percentage of any of the regions we surveyed). This represents a slight drop of eight percent from the 2007 survey, but indicates that KYC remediation remains an area of focus. Since our last survey, financial institutions appear to have changed their approach to remediation efforts, with less reliance on a risk-based approach and a greater tendency to review customers either when they open a new account or when there is a change in business scope.

Outlook

Within the region there will be a continued increase in regulatory pressure, particularly on those financial institutions operating within the EU countries or applying to join.
With continued regulatory pressure on AML compliance and high inherent risks of money laundering, financial institutions need to be vigilant in ensuring their AML controls remain in line with regulatory expectations and international practices.
There are clear and significant legal and reputational risks for those financial institutions that do not focus sufficiently on developing, implementing and monitoring a robust AML strategy.

We await with interest the outcome of compliance audits by parties external to the financial institutions to gauge the extent to which AML controls (particularly in regard to PEPs) have been implemented, as few have been assessed externally to date. Finally, we are seeing that firms are requesting assistance in researching the implications of FATCA and understanding the practical consequences for them.

The Middle East and Africa

Kevin West
KPMG in South Africa

Kauzal Ali Rizvi
KPMG in the UAE

AML/CFT remains high on the agenda of financial institutions across the region. Africa faces significant challenges in respect of compliance, especially when dealing with countries where there is no national identity system and proper address verification documentation. Remediating legacy customers to ensure that they are compliant with AML / CFT legislation is not high on the priority list.

The issue of sanctions, and its application, has been playing a more prominent role, with investment being channeled towards customer and payment screening solutions. However, such solutions require the requisite resources to address potential matches generated by these solutions, and skilled resources are few.

Although AML / CFT will remain high on the agenda, the role of the regulators in taking action against those who do not comply will have a significant impact on the level of compliance by financial institutions. Given the recent financial crisis, cost remains a real consideration and its impact will be felt in the area of AML. Future spend in this area will be very focused, specifically in those areas where the risk is perceived to be the highest.

Senior management interest in AML and CTF is rising

The profile of AML within the Middle East and Africa region has risen over the last three years, with 79 percent of respondents claiming their board of directors takes an active interest in AML (up from 54 percent in 2007). This is reflected in the fact that 64 percent said their board of directors met at least quarterly to discuss AML issues (compared to 48 percent in 2007). A further 24 percent of respondents stated that AML was discussed at least on a monthly basis by their board of directors.

Contributing to this rise may be the South African and Nigerian regulators, the Financial Intelligence Centre (FIC) and the Central Bank of Nigeria (CBN), respectively, issuing industry guidance or AML/CFT Regulations. These require financial institutions within their respective jurisdictions to obtain the approval of their Board of Directors for their AML and CFT policies which are reviewed as part of the inspections performed by the regulators. Indeed, KPMG member firms in South Africa and Nigeria have seen an increase in the number of requests from Boards of Directors and senior management to explain specific AML and CFT topics, ranging from a basic idea of what AML and CFT stands for, through to a higher more in-depth knowledge on specific issues such as KYC and sanctions.

The profile of AML within the Middle East and Africa region has risen over the last three years.

In respect of South Africa's Financial Intelligence Centre Act (FICA), both legal and natural persons (including directors and senior management of a financial institution who are responsible for the institution's contraventions or failures) are liable to criminal sanctions for violating FICA provisions. The maximum penalties for offences relating to violations of customer due diligence, record-keeping and reporting requirements are imprisonment for 15 years or a fine of R100 million (approximately USD15 million). The maximum penalties relating to offences regarding the formulation of internal rules, the provision of training and the appointment of a compliance officer are imprisonment for a period not exceeding five years, or a fine not exceeding R10 million (approximately USD1.5 million).

In Nigeria, the recently enacted new Money Laundering (Prohibition) Act (MLPA), which was signed into law on 3 June 2011, makes both legal and natural persons liable to conviction for violation of its provisions. Violations of CDD, record keeping and reporting requirements of the MLPA can attract a maximum prison sentence of three years and a minimum fine of N1million (approximately USD6,500) for individuals, and a maximum fine of N25 million (approximately USD165,000) for financial institutions. Failure of an institution to maintain proper internal controls and create adequate awareness among its staff to combat money laundering, as stipulated by the MLPA, can lead to a minimum penalty of N1million (approximately USD6,500) for the financial institution.

AML remains a significant risk and cost

Eighty-five percent of financial institutions experienced an increase in their AML investment over the last three years. The main reasons given were an increase in external reporting requirements, enhanced transaction monitoring and anti-bribery and corruption activities. The Middle East and Africa was the only region where enhanced transaction monitoring was not ranked as the main driver for the increase in AML expenditure.

Eighty-two percent of respondents expect their AML compliance costs to increase over the next three years. Just under one-third (30 percent) estimated that their costs would increase by between 10 percent and 20 percent, while 44 percent expected costs to rise by between 21 percent and 50 percent.

Outsourcing of AML and CFT functions is not general practice in the region, with 97 percent of respondents stating that they neither off-shore nor outsource. Of these, 78 percent had never considered off-shoring or outsourcing as an option. We do not foresee this approach changing in the near future. One reason for this attitude could be the effort involved in performing due diligence on third party providers in order to ensure satisfactory levels of compliance, and that the meeting of standards set out by group policy can be significantly greater than undertaking the work in-house.

In addition, data privacy and local laws in our firms' experience are one of the main obstacles faced by international financial institutions for off-shoring customer account opening and sanctions screening.

Politically Exposed Persons: the scrutiny intensifies

Identifying PEPs is not a legislative requirement in South Africa, but is incorporated in the guidance notes issued by the regulator which, strictly speaking, do not form part of the Act and supporting regulations. In Nigeria, the AML / CFT Regulations 2009, issued by the CBN, requires financial institutions to have measures in place for determining whether prospective customers are PEPs. The financial institutions also are required to perform enhanced due diligence on PEPs and obtain senior management approval before opening accounts for them. The AML / CFT Regulations specifically request that financial institutions submit monthly returns on all transactions with PEPs to the CBN and the Nigerian Financial Intelligence Unit (NFIU). It is therefore notable that 97 percent of respondents in the region have specific procedures for identifying and monitoring PEPs on an ongoing basis.

Although the South African guidance notes are intended for information purposes only, the Banking Supervision Department (BSD) of the SARB (the supervisory body for banks in South Africa) does check for compliance with them. The Registrar of Banks has also indicated that the Bank Circulars issued by the SARB are not considered to be legally enforceable. Nevertheless, in practice, financial institutions generally do comply with these instruments.

In Nigeria, the CBN also checks for compliance with the AML / CFT related circulars issued by it and imposes sanctions for non-compliance with them.

In Ghana, identifying PEPs is a requirement by law. Ghana's AML regulations state that an accountable institution has to put in place appropriate risk management systems, in addition to the performance of CDD to determine if a prospective customer or beneficial owner is a PEP.

Eighty-two percent of survey respondents stated they found customer screening to be challenging or very challenging, 11 percentage points higher than the average across all of the regions.

Sanctions compliance remains a challenge

Eighty-two percent of survey respondents stated they found customer screening to be challenging or very challenging, 11 percentage points higher than the average across all of the regions.

Within South Africa, the only customer screening required is in terms of section 25 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA), which criminalizes the collection or provision of property with the intention that it is to be used for the purpose of committing a terrorist act. The names of those that have been designated terrorists by the United Nations Security Council under S/RES/1267(1999), often referred to as the UN 1267 list, are noted within the Government Gazette and are circulated to financial institutions.

Despite the FICA in South Africa only requiring screening against UN List 1267, most respondents do screen against the full OFAC and EU sanctions lists, although the additional costs that are incurred are often questioned.

In Nigeria, many banks screen their customers against the UN List 1267, OFAC and EU sanctions lists. In addition, the CBN occasionally circulates names of new terrorists and terrorist organizations to banks and request them to check their customer database and confirm that such names are not among their customer base.

The majority of financial institutions in the region (88 percent) include originator information within their outgoing SWIFT messages in compliance with FATF VII.

Respondents in the Middle East and Africa region are more rigorous than other regions when it comes to the screening and rejection of SWIFT messages with incomplete information. Ninety-one percent of respondents in the region screen all incoming SWIFT messages for incomplete originator information, compared to an average of 73 percent across the regions. Of those financial institutions that do screen for incomplete information, nine out of ten will stop the message, which is well above the 69 percent global average.

The MT202COV SWIFT message was created to ensure that information in respect of the originating and beneficiary parties was included within the SWIFT message. Given that financial institutions within the region are more prone to screen and stop SWIFT messages with incomplete information, it may be no surprise that 70 percent of respondents processed cross-border wire transfers using MT202COV, which is significantly higher than the 50 percent global average.

Eighty-seven percent of financial institutions in the region screen incoming MT202COV messages for incomplete information (14 percentage points higher than the average). Of those institutions that do so, 90 percent stop the message should information be missing.

Banks in the region are more satisfied with the effectiveness of their transaction monitoring

The majority of respondents (albeit a small majority) in the region appear to be satisfied with their transaction monitoring systems. Fifty-two percent rated their system a four on a scale of 1 to 5 (1 being very unsatisfactory and 5 being very satisfactory). Supporting this, 91 percent of respondents stated that they could monitor a single customer's transaction and account status across different business units.

Almost half (48 percent) of respondents stated that they could not monitor a customer transaction across several different countries, however. This compares to a 44 percent average across all of the regions.

Within the Middle East and Africa region, 85 percent of respondents have a formal program for monitoring the effectiveness of their AML systems and controls.

The role of testing the AML systems and controls is undertaken primarily by the compliance function (93 percent of respondents) and internal audit (89 percent of respondents).

The major financial institutions within the region appear to have well-established AML and CFT departments under the direct control of the Money Laundering Compliance Officer (MLCO), with compliance professionals stationed in each business unit throughout the institution. A relatively small number of the smaller financial institutions assign AML and CFT responsibilities to a general compliance officer. These responsibilities will evidently form only a small element of the tasks allocated to the compliance officer.

Within South Africa, recent changes to FICA introduced personal liability for non-compliance with the Act giving rise to a maximum financial penalty of R10 million. As a result, a trend has developed of appointing a full-time resource to look after AML, CFT and sanctions.

In Nigeria, the MLPA 2011 requires financial institutions to appoint compliance professionals at management level at its headquarters and at every branch and local office. The AML / CFT Regulations issued by the CBN also requires that every financial institution appoints an AML / CFT Chief Compliance Officer that will be responsible for the implementation of the financial institution's AML / CFT program. In practice, all banks in Nigeria have a Chief Compliance Officer at senior management level. The same may not be said of non-bank institutions.

Remediation of KYC data is undertaken by the majority of institutions

A risk-based approach to customer identification and verification has been more or less embedded by most of the local financial institutions in the region. Ninety-seven percent of respondents stated that stricter KYC requirements are dependent upon the money laundering risk posed by the customer.

When undertaking a risk assessment of a potential customer, all financial institutions surveyed considered the nature of the customer's business and whether the customer was a PEP.

In our firms' experience, however, not all financial institutions in the region make use of a consolidated risk framework to determine the risk associated with establishing a business relationship with a particular customer. Some incorporate only certain risk elements into an automated client acceptance process, being mainly geographical location and entity type. Other financial institutions have not only followed a risk framework for client acceptance, but have also upgraded their risk matrix several times over recent years in order to ensure that it remains relevant.

Maintaining up-to-date and correct KYC data for existing clients is a regulatory requirement within the Middle East and Africa region. Consequently, 94 percent of respondents claimed to have a program in place to remediate gaps in their customers' KYC information. Forty-five percent of financial institutions surveyed perform an exercise across their entire customer base to obtain missing KYC information, while 30 percent operate a risk-based approach obtaining missing KYC information for their higher risk customers only.

Within the region we see a move away from the standard risk categorizations of high, medium and low being applied to a customer relationship, towards a simpler approach of classifying a customer in terms of the level of due diligence to be applied (i.e., standard due diligence or enhanced due diligence).

South African legislation requires that at least one senior executive (e.g., CFO/CEO/COO etc.) is identified and verified. In Nigeria, the MLPA requires that at least one individual of the corporate is identified and verified while the AML/CFT Regulations have a more stringent requirement, insisting that financial institutions understand the ownership and control structure of a corporate, verify its existence from the companies registry and determine the natural person(s) that ultimately own(s) or control(s) the corporate. Most financial institutions, however, choose to adopt a higher standard and as a result identify and verify a greater number of (or all) directors. This is reflected by the fact that 84 percent of respondents in the region said they identify all directors and controllers of a customer.

Outlook

Due to the deficiencies cited by FATF and GIABA (The Inter-Governmental Action Group against Money Laundering in West Africa) in respect of Nigeria's AML / CFT regime, Nigeria had to enact a new MLPA 2011 and the Prevention of Terrorism Act 2011 with a view to becoming compliant with FATF Recommendations and Special Recommendations. The two pieces of legislation were assented by the President of Nigeria on 3 June 2011. It is expected that the effective implementation of the new pieces of legislation, the AML / CFT Regulations issued by the CBN as well as other AML / CFT related circulars and guidelines issued by other regulatory bodies within their scope of authority would result in the improvement of the AML / CFT regime in Nigeria. However, much depends on how effective the implementation and enforcement will be.

There is no specific requirement in FICA (South Africa) or its regulations that requires financial institutions to identify ultimate beneficial owners or to verify their identities. In some cases, however, the MLFTC regulations require the identification of a variety of persons who own, control, or are beneficiaries of, a customer. These persons, however, may not be the ultimate beneficial owner as defined by the FATF. The reverse is the case in Nigeria, where financial institutions are required to ascertain the ultimate beneficial owners.

Beneficial owners are defined by FICA as those individuals who have at least 25 percent voting rights at a general meeting. Some financial institutions in the region increase the level of compliance for higher risk customers to those individuals who have at least a 10 percent shareholding.

Within the region we see a move away from the standard risk categorizations of high, medium and low being applied to a customer relationship, towards a simpler approach of classifying a customer in terms of the level of due diligence to be applied.

FATF found that there are no explicit requirements in South Africa to understand the ownership and control structure of a customer, obtain information on the purpose of the business relationship or conduct on-going due diligence. They also concluded that there was no specific requirement within South African law or regulation that required financial institutions to identify or verify the identity of beneficial owners.

The regulator has advised that legislation will be updated in the near future to re-focus on the issue of beneficial ownership and to consider who has ultimate control and influence over the entity, rather than on the percentage shareholding held.

Contact us – Global AML leads in KPMG member firms

Africa and The Middle East

Africa

Kevin West
T: +27 11 647 7992
E: kevin.west@kpmg.co.za

Corrie Fourie
T: +27 11 647 7985
E: corrie.fourie@kpmg.co.za

Willie Oelofse
T: +254 (20) 2806000
E: williamoelofse@kpmg.com

Linus Okeke
T: +234 (0) 1 2710539
E: linus.okeke@ng.kpmg.com

The Middle East and South Asia

Karl Hendricks
T: +971 442 48 900
E: khendricks@kpmg.com

Kauzal Ali Rizvi
T: +971 442 48 900
E: kalirizvi@kpmg.com

Americas

Canada

Pamela Johnson
T: +1 613 212 3614
E: pamelajohnson@kpmg.ca

United States

Teresa Pesce
T: +1 212 872 6272
E: tpesce@kpmg.com

Darren Donovan
T: +1 617 988 1833
E: djdonovan@kpmg.com

Latin America

Judith Galván
T: +52 555 246 8783
E: judithgalvan@kpmg.com.mx

Shelley Hayes
T: +52 555 246 8634
E: hayes.shelley@kpmg.com.mx

Luiz Roberto Cafarella
T: +55 11 3245 8331
E: lcafarella@kpmg.com.br

Diego Bleger
T: +54 11 4316 5910
E: dbleger@kpmg.com.ar

Adriano Mucelli
T: +56 2 798 1565
E: aumucelli@kpmg.com

Ignacio Cortes
T: +57 1 618 8000
E: ignaciocortes1@kpmg.com

Asia Pacific

Australia
Gary Gill
T: +61 (0) 2 9335 7312
E: ggill@kpmg.com.au

Jacinta Munro
T: +61 3 9288 5877
E: jacintamunro@kpmg.com.au

Jeremy Allan
T: +61 (0) 3 9838 4571
E: jallan1@kpmg.com.au

New Zealand
Stephen Bell
T: +64 9 3675 834
E: stephencbell@kpmg.co.nz

India
K.V.Karthik
T: +91 (22) 3090 2094
E: kvkarthik@kpmg.com

Malaysia
Sukdev Singh
T: +60 3 7721 3388
E: sukdevsingh@kpmg.com.my

Japan
Chiharu Yamazaki
T: +81 3 3548 5125
E: cyamazaki@kpmg.com

Takumi Hagiwara
T: +81 3 5218 6702
E: takumihagiwara@kpmg.com

Republic of Korea
Yong Soo Park
T: +82 2 2112 0421
E: yongsoopark@kr.kpmg.com

Sang Hyun Lee
T: +82 2 2112 0745
E: slee17@kr.kpmg.com

China and Hong Kong
Grant Jamieson
T: +852 3121 9804
E: grant.jamieson@kpmg.com.hk

Kyran McCarthy
T: +852 2140 2286
E: kyran.mccarthy@kpmg.com

Singapore
Bob Yap
T: +65 6213 2677
E: byap@kpmg.com.sg

Europe

Austria
Gert Weidinger
T: +43 732 6938 2107
E: gweidinger@kpmg.at

Belgium
Els Hostyn
T: +32 2708 4362
E: ehostyn@kpmg.com

Central and Eastern Europe
Michael Peer
T: +420 222 123 359
E: mpeer@kpmg.cz

Denmark
Torben Lange
T: +45 3818 3184
E: torbenlange@kpmg.dk

France
Jean Luc Guitera
T: +33 1 5568 6962
E: jguitera@kpmg.com

Germany
Frank M. Hülsberg
T: +49 211 475 6563
E: fhuelsberg@kpmg.com

Ireland
Laura Burge
T: +353 1 410 2768
E: laura.burge@kpmg.ie

Italy
Giuseppe D'Antona
T: +39 (0) 680 97 11
E: gdantona@kpmg.it

Luxembourg
Eric Collard
T: +352 22 5151 205
E: eric.collard@kpmg.lu

Netherlands
Bart van Loon
T: +31 20 656 7796
E: vanloon.bart@kpmg.nl

Norway
Per A Sundbye
T: +47 4063 9343
E: per.sundbye@kpmg.no

Russia
Alex Sokolov
T: +74 959 378 549
E: alexsokolov@kpmg.ru

Spain
Enric Olcina
T: +34 93 253 2985
E: eolcina@kpmg.es

Sweden
Sofia Hellsberg
T: +46 8723 9823
E: sofia.hellsberg@kpmg.se

Switzerland
Anne van Heerden
T: +41 44 249 3178
E: annevanheerden@kpmg.com

United Kingdom
Brian Dilley
T: +44 (0) 20 7896 4843
E: brian.dilley@kpmg.co.uk

Matthew Russell
T: +44 (0) 20 7694 2097
E: matthew.russell@kpmg.co.uk

Acknowledgements

We would like to thank all of our AML teams for their contribution to the survey, in particular members of the project and editorial team:

Jeremy Allan,	KPMG in Australia
Samantha Ashfield,	KPMG in the UK
Manet Basson,	KPMG in South Africa
Dmitry Chistov,	KPMG in Russia
Ian Colebourne,	KPMG in Russia
David Cox,	KPMG in the UK
Neal Dawson,	KPMG in the UK
Brian Dilley,	KPMG in the UK
Gary Gill,	KPMG in Australia
Jimmy Helm,	KPMG in the Czech Republic
Amy Idun,	KPMG in the UK
Emma Jordan,	KPMG in the UK
Alan Jones,	KPMG in the UK
Simon Mansell,	KPMG in the UK
James Martin,	KPMG in the UK
Linus Okeke,	KPMG in Nigeria
Enric Olcina,	KPMG in Spain
Alexander Oppong,	KPMG in Ghana
Teresa Pesce,	KPMG in the US
Matthew Russell,	KPMG in the UK
Robert Skrzypczak,	KPMG in the US
Alex Sokolov,	KPMG in Russia
Kevin West,	KPMG in South Africa
Giles Williams,	KPMG in the UK
Eleanor Winton,	KPMG in the UK

Contact Us

Global Head of KPMG's AML Services

Brian Dilley
T: +44 (0) 20 7896 4843
E: brian.dilley@kpmg.co.uk

Regional AML leaders

Europe, Middle East and Africa
Enric Olcina
T: +34 93 253 2985
E: eolcina@kpmg.es

Americas
Teresa Pesce
T: +1 212 872 6272
E: tpesce@kpmg.com

Asia Pacific
Gary Gill
T: +61 (0) 2 9335 7312
E: ggill@kpmg.com.au

RR Donnelley I RRD-254818 I September 2011

www.kpmg.com