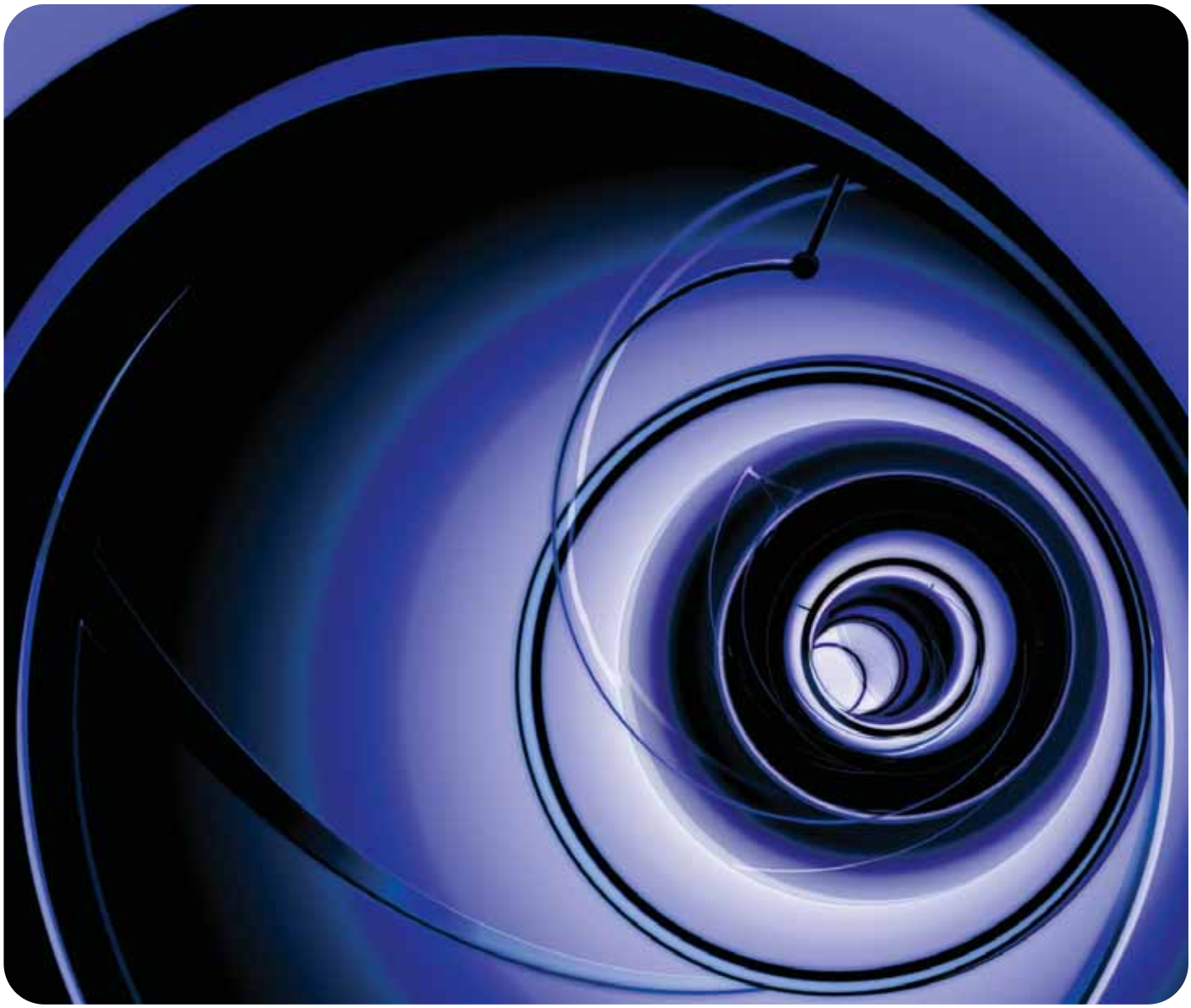
INDUSTRY VIEWS

the journal

Tackling the key issues in banking and capital markets*

June 2006

PRICEWATERHOUSECOOPERS



Contents

PricewaterhouseCoopers

Editor's comments

by Chris Lucas

Chris Lucas

Chairman, Global Banking &
Capital Markets Executive Team

Tel: 44 20 7804 9652
Email: christopher.g.lucas@uk.pwc.com


Welcome to the June 2006 edition of the journal. The past few months have seen some challenging new developments within the global banking and capital markets industry.

The potential impact of the Markets in Financial Instruments Directive (MiFID) on the financial services sector is of such significance that all firms should already be assessing the impact of the proposed requirements on their business. Not only does it present wide-ranging organisational challenges, affecting key areas of the business, but it will also impact the way markets operate. Firms need to consider changes to their internal procedures and systems, and to the procedures by which, and the systems through which, they will interface with the new market structure and other market participants. In our opening article entitled, 'MiFID: European regulation with global impact', Graham O'Connell and Matthew Oswald assess some of the key requirements of the Directive and its impact on business strategy and operations within the banking industry.

The Russian banking sector potentially offers a vast and largely untapped opportunity. With a population of 144 million, increasingly wealthy citizens and over 1,200 commercial banks, it seems Russia's banking sector has a huge potential for profitable growth. Economic growth, higher real incomes and more purchasing power, as well as increasing transparency and market openness are generating significant interest in this country's financial services sector. In our country profile 'Russia's banking sector: Huge growth potential for aggressive players', Rick Munn, Evgeniy Kriventsev and Oleg Mosyazh provide an in-depth analysis of the sector and the potential opportunities, and risks, that exist there.

'Regulators across the world face a range of unenviable challenges in seeking to interpret and supervise Pillar 2, write Richard Barfield, Chris Matten and Shyam Venkat in 'The practical application of Pillar 2: Understanding what supervisors are looking for in a bank's capital assessment'. Regulators' expectations, the views and concerns of industry participants, and the many practical considerations are some of the areas tackled in this article.

Effective compliance reporting is receiving increasing focus within banking institutions, reflecting the profile of compliance risks and issues in recent months. In 'Confident in compliance', Martin Hislop, Jan Willem Kaptein and Alex Shapland explore the principal objectives and management of compliance reporting within a financial services organisation, as well as suggesting the key elements needed in a well-structured and effective compliance-reporting framework.

In 2003, the US Federal Trade Commission found that 215,000 reports of identity theft and fraud had cost Americans at least US$437 million. As identity theft attacks become increasingly more frequent and diverse across the globe, in 'Does identity theft affect your organisation?', Mark Vos, Jan Schreuder and Philip Riley look at how identity theft is threatening the banking industry and explore practical measures organisations can take now to protect themselves against the risks.

I hope you find this edition of the journal of interest. Please do continue to provide us with feedback on the topics you would like to see addressed in future editions.

PRICEWATERHOUSECOOPERS

The Markets in Financial Instruments Directive: European regulation with global impact

by Graham O'Connell and Matthew Oswald

Graham O'Connell

Director, Financial Services Regulatory Practice, UK

Tel: 44 20 7212 3826
Email: graham.r.oconnell@uk.pwc.com

Matthew Oswald

Senior Consultant, Financial Services, UK

Tel: 44 20 7804 4230
Email: matthew.c.oswald@uk.pwc.com

Why is MiFID important?

The Markets in Financial Instruments Directive (MiFID) is one of the most significant pieces of Financial Services legislation to be enacted by the European Parliament to date. It will result in a radical change to market dynamics in all investment sectors and will require market participants to take fundamental strategic decisions in order to establish an effective operating model in the post-MiFID world. Wholesale and retail markets will both be significantly affected and for individual firms the impact will be felt in Trading, Research, Fund Management, Operations, Settlements and Compliance. Above all, the effectiveness of a firm's approach to assessing the impact of MiFID and implementing the required changes will have a direct effect on the firm's future effectiveness and profitability.

The objective behind the regulation

MiFID is a cornerstone of the European Union's aim to develop a single European securities market with common standards. MiFID itself is a harmonised set of Conduct of Business requirements which covers all investment products (see Figure 1) and services (see Figure 2) and establishes rules around governance, trading, risk, compliance, operations, systems, customer documentation and outsourcing (see Figure 3). The main objectives are increasing price transparency in the markets; increasing awareness of risk amongst customers; and promoting greater competition amongst execution venues. The EU has deliberately set out to create a framework which will affect the way that business is conducted and change the dynamic of investment markets. It is for this reason that MiFID should not be considered as a 'compliance' issue, but as a far more fundamental driver for business change in investment firms and markets.

A new equity market structure

In equity markets, MiFID will sweep away the current concentration rules that require trading to be carried out over national exchanges, and will further open up cross-border trading. In order to

Figure 1: Investment products covered

- Transferable securities
- Money market instruments
- Units in collective investments
- Options, futures, swaps and any other derivative contracts related to securities, interest rates or yields
- Options, futures, swaps and any other derivative contracts related to commodities that may be settled in cash
- Options, futures, swaps and any other derivative contracts related to commodities that may be settled physically and are traded on a regulated market or MTF
- Options, futures, swaps and any other derivative contracts related to climatic variables, freight rates, emission allowances or inflation rates that may be settled in cash
- Financial contracts for difference
- Derivative instruments for the transfer of Credit risk

Source: PricewaterhouseCoopers

Figure 2: Core investment services covered

- Reception and transmission of orders
- Execution of orders on behalf of clients
- Dealing on own account
- Portfolio management
- Investment advice
- Underwriting and/or placing of financial instruments
- Operation of Multilateral Trading Facilities

Source: PricewaterhouseCoopers

Figure 3: Some key requirements of MiFID

- All customers must be reclassified
- New customer agreements required
- Determine 'Best Execution' for all investment products
- Some firms required to provide public quotes for order-matching
- Firms to establish a Compliance function and effective compliance procedures
- Firms to establish Risk and Internal Audit functions based on complexity of business
- Document and assess the quality of 'Execution Venues'
- Obtain customer agreement to Execution policy
- Establish effective Conflicts of Interest procedures
- Carry out revised transaction reporting to regulators
- Inclusion of derivatives within EU legislation for the first time
- Inclusion of investment advice within EU legislation for the first time
- More stringent outsourcing requirements inside and outside the EU
- Rules established for 'Multilateral Trading Facilities'

Source: PricewaterhouseCoopers

maintain a transparent market for end users, MiFID will require those firms that currently match customer orders within their own organisation, to publish pre-trade prices and then publish post-trade data. The firms that currently do this on a systematic basis with staff and systems that are dedicated to this activity will be known as Systematic Internalisers (SI) and will begin to be treated in a similar way to Recognised Investment Exchanges and their on-line counterparts Multilateral Trading Facilities (MTFs).

Multilateral Trading Facilities (MTF) and Systematic Internalisers (SI)

These changes mean that execution will no longer be centred around national exchanges but will gravitate to the most price efficient execution venues with the greatest liquidity. As well as the inevitable competition between exchanges and investment banks, the role of the order matching systems (MTFs) will become more prominent. It is already clear that a number of investment banks will establish their own MTFs to reduce costs and increase efficiency for their own clients. As a result of the increased number of execution venues, price publication is likely to become far more fragmented. In order to address this, MiFID itself anticipates that there

will be a market-led solution to the consolidation of price reporting. Consequently, there will be increased competition amongst data vendors, MTFs, exchanges and investment banks to establish themselves as the accepted source of centralised price publication and trade data.

How to demonstrate Best Execution

Another significant issue in trading all investment products under MiFID will be the need to demonstrate 'Best Execution'. Even in equity markets, the need to consider price, cost, speed, reliability and likelihood of execution in relation to the nature of the order and the nature of the client will prove challenging. To do so in illiquid or open outcry markets will be extremely difficult and this is an area that will require an effective market solution which brings regulators along with it. There is also a concern that there may not be a consistent approach in the application of this requirement for all jurisdictions. Whilst some regulators may take a broad approach to this issue based on a generic policy issued by the firm, others may require firms to demonstrate adherence on a trade-by-trade basis, which will prove costly and unwieldy.

The effect of MiFID on Buy Side firms

A key objective of MiFID is to increase awareness of risk and improve transparency in the trading and advice process. Consequently, all investment firms dealing with customers will need to retain more customer documentation including revised customer agreements, enhanced 'Know Your Customer' data, more information on trading costs and post-transaction reporting. Customers will be asked to agree to the firm's execution policy and must also be advised where a firm is not 'reasonably confident' that its conflict management process will be effective in a specific instance. In addition, firms will be required to reclassify all their customers and must give those customers the option of changing their classification in specific circumstances. Whilst this is intended to empower customers to a greater extent, many firms feel that customers will take a negative view of the additional paperwork and data requests.

The effect outside the EU region

Many of the firms that will be most affected by these changes are global businesses with 24 hour trading books and worldwide systems and processes. The introduction of MiFID will require these firms to either change global systems and controls to address European regulation, or else they will need to decouple their global processes and establish stand-alone systems and procedures for their European operations. In addition, there are certain aspects of the new rules that may be seen as 'extraterritorial', requiring the MiFID rules to be addressed outside the EU region. In particular, the outsourcing rules will mean that EU investment firms that outsource any 'critical or important operational functions' to a service provider in a 'third country' may only do so if the service provider is regulated in that country and is subject to prudential regulation. Even then there will need to be a co-operation agreement between the investment firm's regulator and the service provider's regulator.

Implementing a common standard

In order to create a level playing field, much of this Directive will be implemented as 'regulation', meaning that national regulators will have very little opportunity to interpret the EU requirements to fit their local market conditions. Therefore, even in territories where many of the MiFID concepts already exist, the local regulator will

The Markets in Financial Instruments Directive: continued

largely have to replace existing rules with the MiFID rules. The result will be that investment firms in all EU territories will have to carry out a significant amount of work across the business to demonstrate that they meet these new requirements.

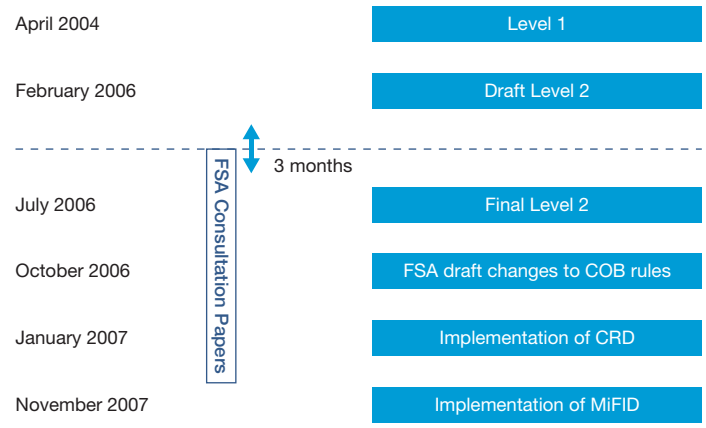
The key stakeholders in the business

The MiFID requirements are wide-ranging and will require input from most areas of the organisation. Typically, effective steering groups within investment firms include Heads of Compliance, IT, Trading and Operations as a minimum, with representation at Board level. As MiFID projects develop, firms will need to develop a broader awareness-raising process to ensure that all business heads understand the effect that this Directive may have on their day-to-day processes. The ultimate objective will be to turn MiFID from a detached project into an embedded part of the 'business as usual' process.

The timetable for implementation

The known dates at present are that the original Directive was ratified in April 2004 and the final implementation date is still intended to be 31st October 2007. The EU implementation documents (the 'Level 2' documents) were published on 6th February 2006 and are still being ratified by Parliament. Thereafter it is expected that national regulators in EU Member States will translate the EU requirements into national rulebooks during 2006. The scale of the changes required, particularly in relation to systems and in obtaining customer documentation and legal agreements, means that the final implementation date does not give investment firms much time to become fully compliant.

Figure 4: Timetable for implementation



Source: PricewaterhouseCoopers

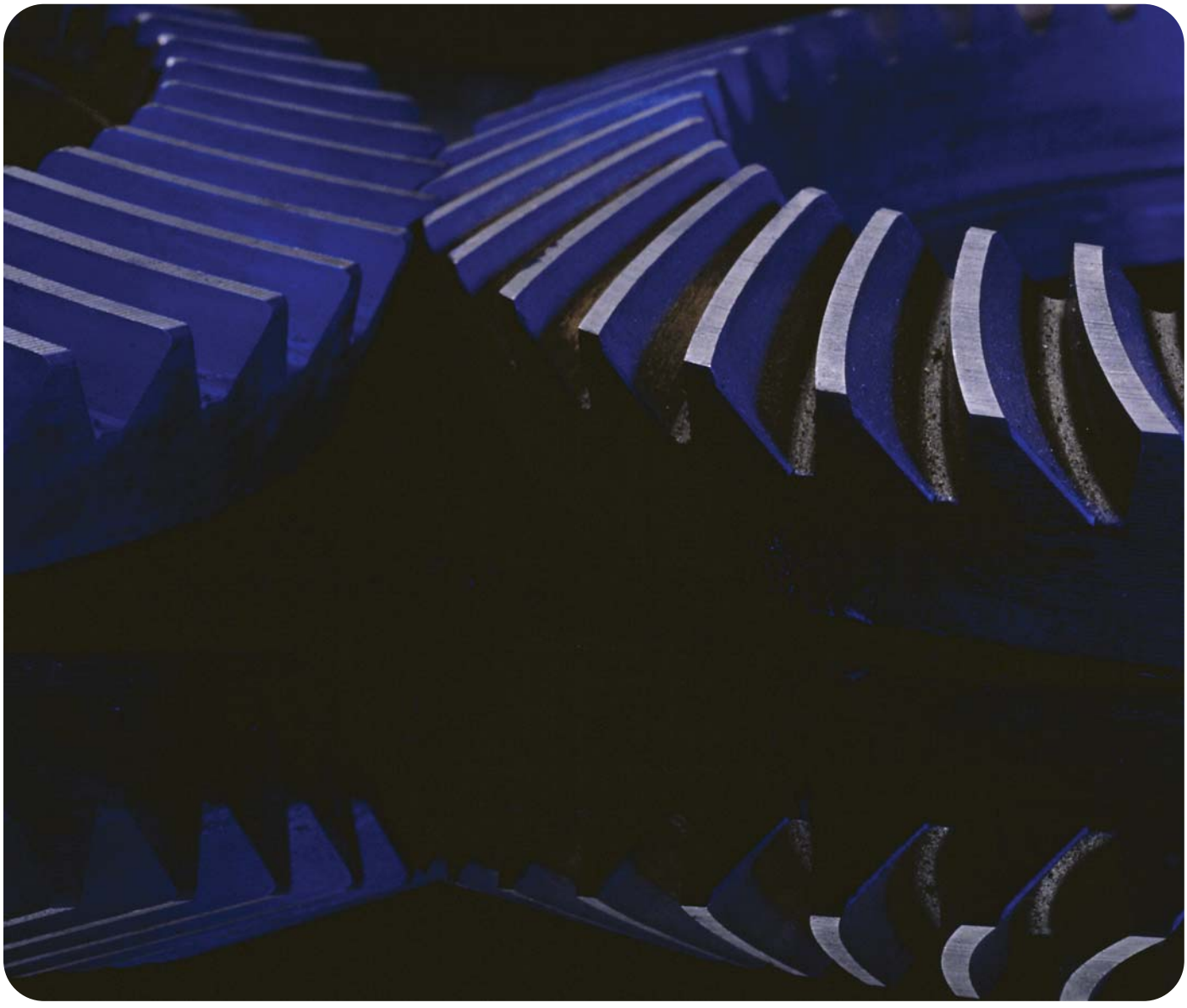
An effective approach to MiFID

Given the resource intensive nature of MiFID, there is clearly a 'first mover' advantage, with those firms that identify key issues for their business at an early stage likely to emerge as the best placed to minimise disruptions and maximise opportunities. Therefore firms should now be assessing what impact the MiFID requirements will have on their business and on the markets they trade in, and putting in place an effective implementation plan, prioritising those areas of greatest strategic advantage.

PRICEWATERHOUSECOOPERS

Russia's banking sector: Huge growth potential for aggressive players

by Rick Munn, Evgeniy Kriventsev and Oleg Mosyazh



Rick Munn

Industry Leader, Financial Services, Russia

Tel: 7 495 967 6342
Email: rick.munn@ru.pwc.com

Evgeniy Kriventsev

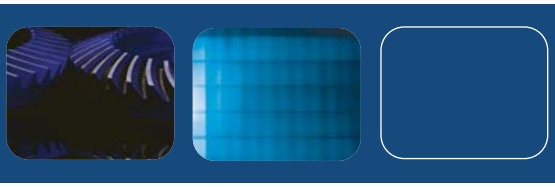
Senior Manager, Financial Services, Russia

Tel: 7 495 967 6373
Email: evgeniy.kriventsev@ru.pwc.com

Oleg Mosyazh

Manager, Financial Services Marketing, Russia

Tel: 7 495 967 6074
Email: oleg.mosyazh@ru.pwc.com



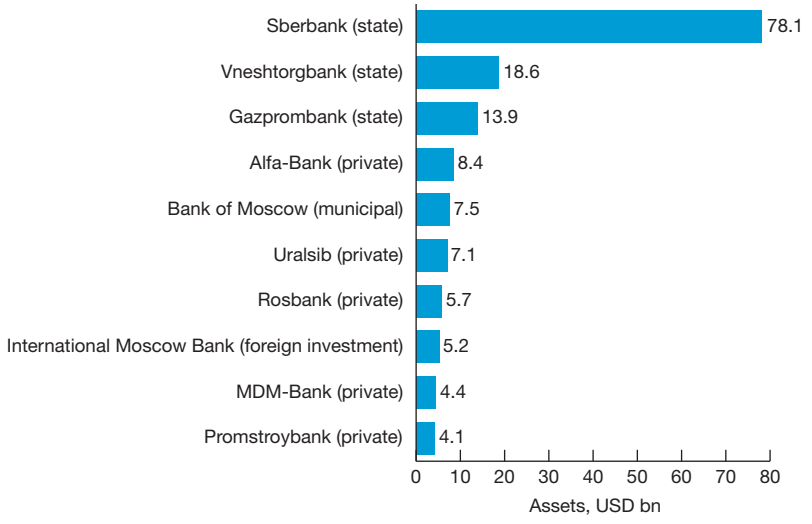
The Russian economy has been growing over the last six years by more than 6% a year, faster than not only developed countries, but also most other emerging markets. Individuals' income is also growing, stimulating a boom in consumer demand. Undoubtedly, this growth requires a corresponding improvement in the country's financial sector. In this article we review the Russian banking sector, analyse current trends and focus on the key factors affecting its development.

The Russian banking sector

Russia has just over 1,200 commercial banks. At the end of 2005, total assets of the banking system exceeded $300 billion, and share capital approximated $40 billion. The Russian banking sector is highly consolidated, with the 100 largest banks accounting for over 80% of total assets and 70% of capital (see Figure 1).

State banks traditionally hold a strong position, owning over half of all assets. The largest (by asset volume) privately owned Russian bank, Alfa-Bank, is only the fifth largest in the country.

Figure 1: Top 10 Russian banks by assets



Source: Interfax, PricewaterhouseCoopers

The dominant bank is state-owned Sberbank, founded in 1841 and previously the monopoly retail bank during the Soviet era. Sberbank is the largest financial institution in central and eastern Europe, accounting for over 25% of all the assets and capital in Russia's banking system. Sberbank dominates the retail banking market, holding around 60% of all retail deposits and issuing over 40% of all retail loans. The dominating presence of Sberbank is due to a long-standing association with the state, historical general public loyalty, and over 20,000 branches located not just in every city of the country, but also in many villages where there are simply no other banks.

Russia's banking sector continued

The Central Bank

The Central Bank of the Russian Federation is the main regulator of the banking sector. In addition to its supervisory and licensing role, the Central Bank also sets out the rules and procedures for making bank transactions, the reporting requirements for banks and rules for making settlements in Russia. It is also responsible for many aspects of monetary policy of the Russian Federation.

Growth potential

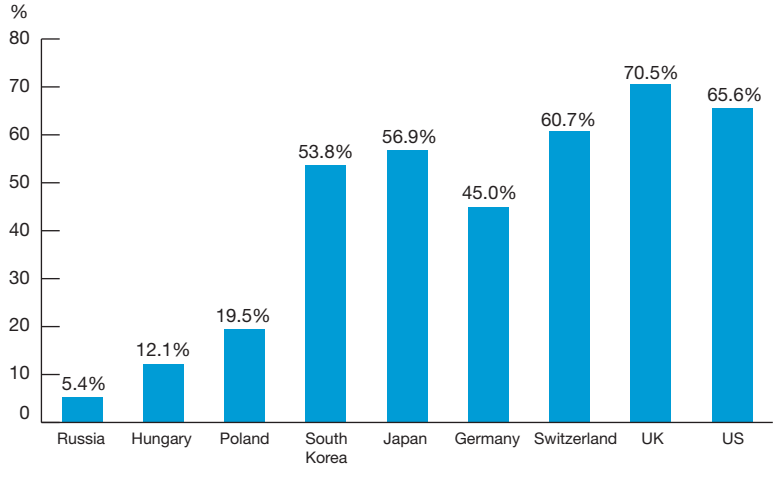
Even though the Russian banking sector has seen rapid growth in retail lending, the retail lending share in GDP in Russia at the beginning of 2006 was only 5% – far behind that in developed countries (around 50% in Eurozone countries, over 65% in the USA and over 70% in the UK). To further illustrate, the share of mortgage lending in GDP in Russia is as low as 1% (55% in the USA and over 30% in Eurozone countries). Given the current boom in retail banking, this gap between Russia and developed countries will clearly shorten (see Figure 2).

Another growth area for the banking sector is the introduction of new banking products and services. For example, despite the relative popularity of plastic debit cards, of which there were 47.2 million by the third quarter of 2005, banks only began offering credit cards to individual customers in 2005. Overall, plastic in Russia has limited use: 94% of operations are used for cash withdrawals, while in European countries 50% of plastic card operations are to pay for goods and services.

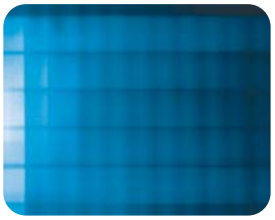
Retail banking boom

Economic growth, higher real incomes and, consequently, more purchasing power are having a positive effect on retail banking in Russia. Close to $100 billion worth of retail deposits was recorded by the end of 2005 – equal to around one third of total liabilities in the Russian banking system. While the share of retail deposits as a percentage of total liabilities of Russian banks has remained relatively stable since the beginning of 2003, the share of retail loans as compared to total assets grew almost three times over the same period from 6.6% to 17.5%. In monetary terms, the growth of retail lending is even more impressive: from $3.6 billion outstanding in early 2003 to $40 billion outstanding in early 2006. In the third quarter of 2005, growth of retail loans outgrew growth of retail deposits for the first time and this trend will most likely continue over the next couple of years.

Figure 2: Retail loans to GDP ratio (%): Russia vs. selected economies



Source: EIU, ECB, CEIC, CBR



PricewaterhouseCoopers estimates that over 1.7 million cars were sold in Russia in 2005, totalling $22 billion in value. Although in unit terms this was only a 7% rise on the figures for 2004, the cost of the cars bought grew by 21%. One factor for this growth was better car loans. According to different estimates for 2004, 15–20% of car sales with, total value of $2.7–3.7 billion were made on credit, while in 2005 the share of cars sold on credit grew to 25–28% and reached $5-6 billion. Motor industry figures and analysts forecast that up to 60% of cars will be sold on credit in 2008–2009.

Experts estimate that Russian mortgage lending is more than doubling each year. If, at the beginning of 2005, mortgage loans totalled $2 billion, experts believe that the $20 billion threshold will be broken by 2008. The main factors preventing faster development of this type of lending are relatively high interest rates at between 9% and 14%, and a high initial own investment requirement of at least 20% of the property value.

An explosive growth of retail lending may affect the quality of credit portfolios of the banks. Currently, relatively high-loan losses on retail loans are compensated by high interest rates. Banks generally obtain above the market margin on lending to individuals.

Thin capitalisation

Thin capitalisation of Russian banks is a key problem, which could slow down the further development of the banking sector and its growth rate. The Central Bank requires strong compliance with its regulatory requirements, including capital adequacy ratios. From time to time this imposes certain limitations on the business of even large Russian financial institutions. At the same time, large local investors are often relatively relaxed about making significant investments in the banking business since investments in natural resources extraction, retail and consumer sector, currently provides them with higher returns. Foreign investments into the Russian banking are still quite limited. Therefore, Russian banks are actively looking for alternative solutions to capitalisation problems, including international placements of subordinated loan participation notes.

International financing

Increased transparency and stability of the Russian banking system has allowed Russian banks some access to longer and less expensive international financing.

Eurobonds are still the most popular mechanism among Russian banks for attracting funds, bringing tens of billions of dollars at 7–8% into the Russian banking system, in 2005. Generally, Eurobond issues were for between $150 and $500 million, but several large banks, such as Sberbank, Gazprombank and Vneshtorgbank, had a range of bond issues worth over $1 billion.

Asset securitisation is still relatively new for Russian banks, and due to undeveloped related legislation in Russia, market players have to issue asset-backed securities on foreign exchanges. For example, Bank Soyuz, which in 2005 made the first Russian securitisation of its car loans for $50 million and Home Credit & Finance Bank (HCFB), which made the first Russian securitisation of rouble-denominated consumer loans. Both these transactions were placed abroad, on the Irish Stock Exchange.

Even though a lot of activity was seen from Russian companies in 2005, attracting more than $10 billion through public floatations, so far no Russian bank has made an initial public offering (IPO). Yet many banks have already announced their plans to float shares in 2006, including the large Vneshtorgbank and Rosbank.

Foreign capital

With 89 federal regions, 144 million citizens with growing incomes, 13 cities with a population of over 1 million and 168 cities of over 100,000 people, Russia is an attractive market for foreign players.

Russia's banking sector continued

There are 133 credit organisations with foreign participation in Russia. International credit organisations are increasingly interested in the Russian banking sector. In 2005, the number of banks with 100% foreign capital rose from 33 to 42. Simultaneously, the share of foreign capital in the Russian banking sector also grew. If in early 2005 foreign banks' share was less than 8%, in January 2006 it was over 11%, according to the Central Bank statistics. However, banks with foreign participation are not among the leaders in Russia at the moment. Only three banks with foreign capital featured in the top 20 Russian banks, by assets, as at 1 November 2005: International Moscow Bank, Raiffeisenbank Austria and Citibank, occupying eighth, eleventh and fifteenth places, respectively.

Recently, foreign banks have stepped up acquisitions of stakes in Russian banks. The most visible recent deals were; GE Consumer Finance's acquisition of Deltabank for $100 million in 2004; Banca Intesa's (Italy's No. 1 bank by assets) purchase of a controlling stake (75% minus one share stake) in KMB-Bank for $90 million in 2005; Société Générale's purchase of DeltaCredit for $100 million in 2005; Dresdner Bank's purchase of 33% of Gazprombank for $800 million in early 2006; and Raiffeisenbank's acquisition of Impexbank for $550 million, announced in February 2006. We are sure to see several more such deals in the near future.

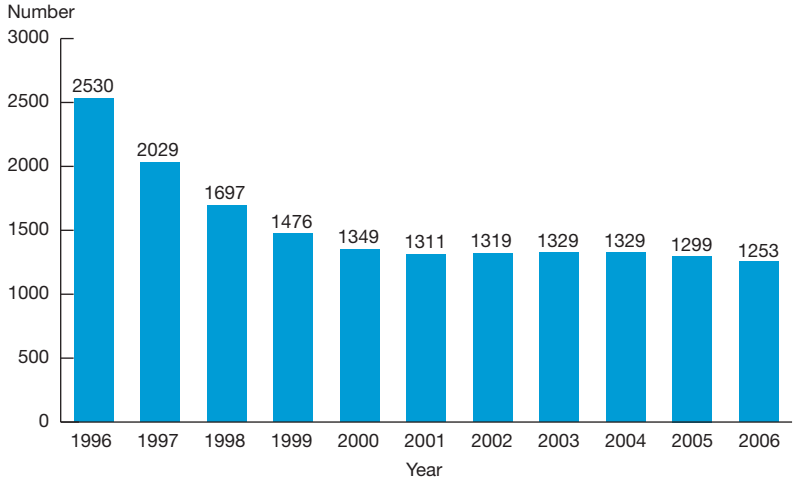
One of the most active investors in the Russian banking sector is the European Bank for Reconstruction and Development (EBRD). It currently has holdings in 23 Russian banks, mainly investing in the share capital of regional banks. Its investment level in 2004–2005 was around $500 million per year and according to statements by the bank's representatives, it will stay around that level in 2006.

Consolidation and regional expansion

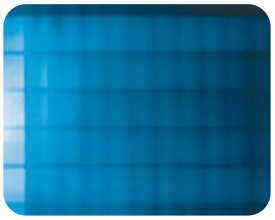
More regulation, tougher competition and increased capital requirements in the financial services market have steadily cut down the number of banks in Russia over several years. In 1996, Russia had 2,538 banks; 1,253 banks held licences for banking operations in 2006 (see Figure 3).

Along with foreign banks purchasing stakes in Russian banks, Russian banks are also active in the mergers and

Figure 3: Number of banks in Russia: 1996–2006



Source: CBR



acquisitions (M&A) market. Mainly, these are national banks, which buy regional banks to enter local markets. However, there is an opposite trend: several regional banks that have outgrown their initial markets, strive to reach a nationwide status via organic growth and through M&A.

Transparency

In late 2005, the international rating agency, Standard & Poors, made a survey of transparency in 30 of the largest Russian banks, mainly on the basis of publicly available information. The study showed a low level of publicly available information, when compared with similar foreign credit institutions. The average level of disclosure by Russian banks in the study was only 36% (85% for the largest foreign banks). To raise the confidence of depositors, investors and the public, in general, Russian banks need to make significant progress on information disclosure in the next few years.

Russia's entry to the WTO

By 2006, Russia had reached agreement with almost all WTO member countries on its entry to the WTO. As it stands, in early 2006, Russia is still negotiating with three countries: the US, Australia and Columbia. The main point of debate in negotiations with the US is foreign commercial banks opening branches in Russia. Russia does not want to lift its ban on foreign bank branches and is 'sticking to its guns', arguing that the risk of losing control of monetary flows in the country is too high. At the same time, there are currently no formal obstacles for foreign banks to operate in Russia through resident subsidiaries.

Conclusion

In the current conditions of an emerging economy and growing wealth of citizens, Russia's banking sector has a great potential for profitable growth. Retail and regional expansion, higher capitalisation, new banking products and services, more transparency and implementation of new technologies are the key success factors for the financial institutions looking for dynamic profitable growth in Russia. Who will win? What are the risks? What are the returns? Only the future will show. However, as with virtually everything in Russia – the growth potential is huge, but one has to be aggressive to make a decent return.

PricewaterhouseCoopers

The practical application of Pillar 2:

Understanding what supervisors are looking for in a bank's capital assessment

by Richard Barfield, Chris Matten and Shyam Venkat

Richard Barfield

Director, Valuation & Strategy, UK

Tel: 44 20 7804 6658
Email: richard.barfield@uk.pwc.com

Chris Matten

Partner, Banking and Capital Markets Industry Group, Singapore

Tel: 65 6236 3878
Email: chris.matten@sg.pwc.com

Shyam Venkat

Partner, Advisory, Financial Risk Management, US

Tel: 1 646 471 8296
Email: shyam.venkat@us.pwc.com


The fog enveloping the practical application of Pillar 2 of the Basel II framework is beginning to clear. Over the last few months, regulators including the UK Financial Services Authority (FSA) have been developing their approach to assessing a bank's process for linking its capital to its risk profile. The FSA is arguably one of the most advanced in its thinking on this issue and the FSA's lead provides banks with useful insights into what other supervisors may expect under Pillar 2.

Spare a thought for the regulators. Regulators across the world face a range of unenviable challenges in seeking to interpret and supervise Pillar 2. These include the translation of qualitative risk assessments into quantitative capital requirements. More broadly, they must decide how to strike the right balance between providing appropriate guidance and being suitably non-prescriptive in keeping with what is a principles- rather than a rules-based framework. Such hurdles need to be overcome in order to oversee an industry that ranges from large, international banks to small mutual societies, stockbrokers and asset managers, and whose firms have diverse approaches to managing risk and capital.

The regulators' approach matters for banks because the supervisor's role is to form a view on an appropriate Pillar 2 buffer above the Pillar 1 capital minimum. For some institutions this is likely to be a significant amount of additional capital. The key input to this assessment will be the bank's Internal Capital Adequacy Assessment Process – the ICAAP[1]. In developing its approach to Pillar 2, the UK FSA has expressed certain expectations regarding a firm's ICAAP.

For many institutions, economic capital will have a role to play. A survey of more than 200 banks and other financial services firms from around the world, which was carried out for the recent PricewaterhouseCoopers/Economist Intelligence Unit (EIU) briefing on economic capital, found that 44% of the participants already use it and a further 13% plan to implement it in the next year[2]. The same report noted that 50% of the world's top 50 banks already include economic capital disclosures in their annual reports (this is up from just over 20%, four years ago).

What the FSA expects

The key principles underpinning the FSA's approach are that supervisory guidance will be kept to a minimum and that the ICAAP should reflect what the firm does for its own purposes (see Figure 1 overleaf). These same principles apply in the CEBS guidance to supervisors in the European Union (EU). As such, the FSA does not make economic capital a specific requirement. However, it does insist that the ICAAP should be a core management tool and therefore a firm is likely to come unstuck if it treats its ICAAP as purely a regulatory exercise.

The onus will be on the institution to convince regulators that it holds sufficient capital for the risks that it runs within the context of its strategy and the external environment. To decide whether they are convinced, regulators will undertake desk reviews and site visits and engage in dialogue with management. While the numbers will of course be important, the demonstrable rigour of the ICAAP process in its own right and its integration into the management of the institution are likely to be equally of interest to the regulators.

1 This is the acronym adopted by the Committee of European Banking Supervisors (CEBS) to describe this part of Basel II
2 'Effective capital management: Economic capital as an industry standard?' (www.pwc.com/financialservices)

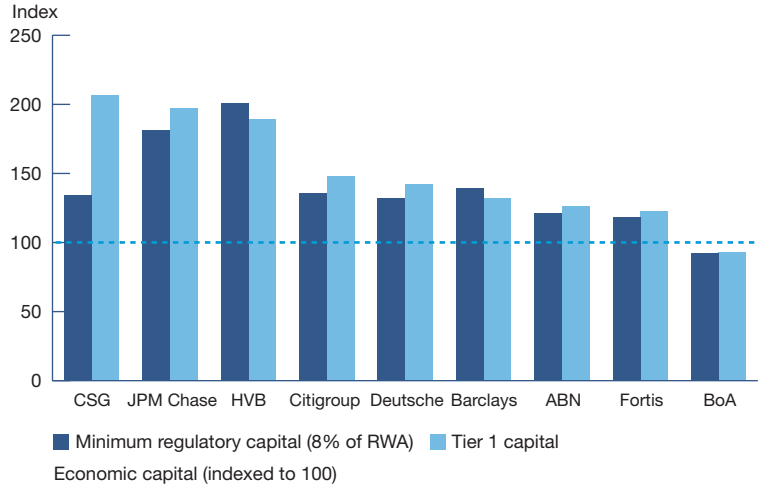
The practical application of Pillar 2: continued

Figure 1: FSA expectations of a firm's ICAAP

- Clearly described and evidenced ICAAP process
- Comprehensive coverage of material risks
- Quality of management and track record of delivery
- Business as usual capital
  - Conservatism in Pillar 1 and Pillar 2
  - Perspective of how it will behave through a cycle
- 'Simple and intuitive presentation'
  - Clear top-down view
  - Clear statement of assumptions
  - Differences between Basel II and risk capital for Pillar 1 risks

Source: FSA presentations November 2005

Figure 2: Relative capital levels



Source: 2004 company accounts, analyst presentations and PwC analysis
Note: The Bank of America comparator figures appear low due to high economic capital at year-end 2004 as a result of the merger with Fleet First Boston.

Lingering challenges

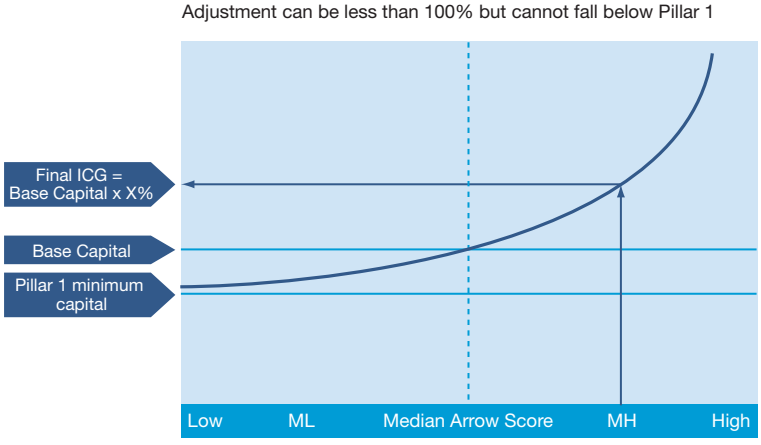
One challenge for regulators will be to decide how to make valid peer comparisons when risk capital frameworks vary so much between particular institutions. The difficulty in establishing comparable figures means that judgement will inevitably play a major role in benchmarking capital levels. An analysis of the public disclosures of economic capital by the world's largest 50 banks brings home this point as well.

Under current conditions capital adequacy does not appear to be an issue. PricewaterhouseCoopers analysis of the disclosures from the nine users of economic capital in the top 20 global banks show that at the end of 2004 they held significantly more Tier 1 book capital than economic (risk) capital – see Figure 2. Three of the nine carried practically double their economic capital in terms of Tier 1 (a proxy for shareholders' funds). Their economic capital was also significantly less than minimum regulatory capital under the cruder measure of 8% of Basel I risk weighted assets. (For smaller institutions the gap may be narrower because they tend to be less diversified and therefore more risky).

However, there is no standardised approach to economic capital calculations. So even though around half of the world's largest banks now disclose economic capital figures in their annual reports, the numbers are more useful in assessing the trends in individual institutions than in making benchmark comparisons. The problem is illustrated by the difficulties in making comparisons using the longer established Value-at-Risk disclosures. Differing holding periods, confidence levels, modelling approaches and correlation effects all conspire to mislead the unwary. Depending on the model and assumptions used, the same portfolio can give quite different but equally valid results. This is compounded in the case of economic capital as it is not always clear what this should be compared with – should required economic capital be compared with available Tier 1 capital? Or shareholders' funds? Or tangible common equity, or any other definition of capital?

A second major challenge for regulators will be linking the qualitative measurement of risks, controls, governance and mitigants (which the UK FSA assesses through its Arrow process) to capital adequacy assessments. Figure 3 shows schematically how the FSA expects this to operate. If the score is high (that is, bad from a firm's perspective), this will be reflected in the size of the buffer over

Figure 3: Linking the qualitative assessment to capital estimation



Source: FSA presentations November 2005

Pillar 1. As mathematicians will remember, if you examine a curve in magnified detail, it actually appears as a series of very small steps. It will be interesting to see how marked the steps turn out to be in practice. At another extreme, one other non–EU national regulator is rumoured to be considering a simple flat percentage add-on to Pillar 1 as the way to estimate the capital buffer – independent of risk assessment. Although simplicity is appealing, how would such an approach allow the regulator to reward firms with superior risk management? And how does it provide an incentive for firms to make a rigorous assessment of their own capital needs?

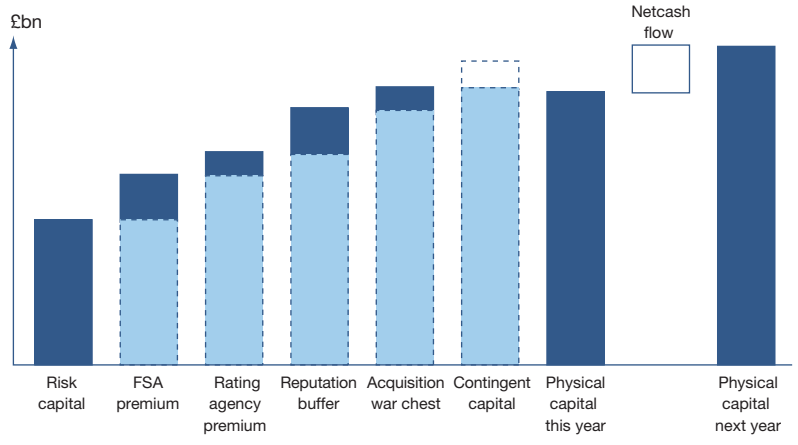
Industry perspectives

The FSA and the UK banking industry have been engaged in dialogue for a while over the right approach to Pillar 2. This means that both the FSA and the industry should have a good understanding of each others' perspectives – even if they do not always agree.

Banks hold capital for many reasons and risk capital is just one component. (Figure 4 overleaf shows the key components). The capital management process in an institution will address all of these elements. A bank also needs to consider, for example, rating agency

The practical application of Pillar 2: continued

Figure 4: The business perspective on capital management is much wider than regulation



Source: PricewaterhouseCoopers

requirements; how much safety buffer it wishes to hold to protect its reputation; capital for acquisitions, and so on.

The expectations and concerns of industry participants regarding Pillar 2 will of course vary depending on where they stand. One could reasonably expect banks whose economic capital is lower than Pillar 1 capital to argue strongly that their regulatory capital under Basel II should be less than Pillar 1. This is because most economic capital models cover many additional risks other than the three covered by Pillar 1: market, credit and operational. However, under the new Basel accord, Pillar 1 is a minimum capital requirement. An important counter-argument from regulators will be that the models are relatively new – many have not be tested through sharp economic changes – and that a degree of conservatism is needed, particularly when the comparative economic capital results are predicated upon correlation assumptions that are not easily observable.

At a high level, common industry expectations are that the FSA's assessment of an ICAAP should incorporate:

- a 'business-as-usual' view of capital calculations and management processes (that is, not forced unnecessarily to fit doomsday regulatory scenarios);
- a sensible allowance for diversification benefits (these can be between 20-40% of capital for a diversified institution); and
- consideration of total capital and not just core equity (there is often a tendency to focus on Tier 1 capital whereas other forms of capital are important ingredients in the capital structure of sophisticated institutions).

Concerns will also vary from institution to institution. At a high level, the main industry misgivings over the FSA's approach include a reluctance to see:

- a requirement for one-off ad hoc exercises prepared largely for the regulator;
- conservatism for its own sake in capital estimation (many believe that the Basel II formulae already include adequate conservatism in the calculation of Pillar 1 capital); and
- stress tests used to determine additive capital estimates (the view being that stress tests test the resilience of capital).

The main underlying concern, however, is that the banks are unsure how they will meet the FSA's requirements when these have not been fully spelt out. Unfortunately, they are unlikely to be spelt out – as Pillar 2 is principles-based, detailed guidance cannot be expected. Desire on management's part for detailed rules is unlikely to be satisfied.

One non–EU supervisor used a 'Dear CEO' letter last year to suggest to its major banks that they should adopt economic capital and described in some detail how it should be applied. Understandably there was strong industry push-back. In their view, the regulator had strayed too far into internal management matters. Within the United States, regulatory agencies such as the Federal Reserve have led the way in suggesting the adoption of economic capital programmes to constituent banks. However, such encouragement has stopped short of prescriptive guidance.

Our advice to clients is to adopt a principles-based approach themselves and focus on addressing the following practical issues. Are all material risks covered? Is there clear ownership of risks? Is it clear which risks are best addressed through capital (e.g. interest rate risk in the banking book) or through controls and mitigation (for most banks this would include reputational risk)? Are controls appropriate and adequate? Figure 5 illustrates how a range of approaches is essential. Are risk and capital sufficiently inter-linked? One of the bigger challenges facing firms that have traditionally used a regulatory capital model to underpin internal capital management is the switch to determining their own internally derived risk capital levels, rather than reading off Basel I formulae.

Once the risk capital framework has been validated there is plenty of detail with lots of devils lurking therein. One particular area that will be of increasing importance is stress testing, given the judgements that are necessary to estimate risk capital figures. The design and application of effective stress tests to demonstrate the resilience of capital in adverse circumstances will be essential to inform the intuitive top-down assessment that most regulators will be seeking to apply.

Figure 5: Risk and capital approaches

Risk type	Capital model	Controls/mitigants management action	Stress tests
Market	✔✔✔	✔	✔
Credit	✔✔✔	✔✔	✔
Operational	✔✔	✔✔	✔
Business	✔✔	✔	✔✔
Reputation	–	✔✔✔	✔
Liquidity	✔	✔✔	✔✔
Interest rate risk	✔✔✔	✔	✔

Source: PricewaterhouseCoopers

The practical application of Pillar 2: continued

Onus on firms

The move from a formulaic capital calculation to risk- and principles-based prudential regulation marks a sea change for banks. Pillar 2 of Basel II puts the burden of proof firmly on firms themselves to convince the regulator that they hold sufficient capital. A key part of the 'evidence' will come from demonstrating the thoroughness of the process and ensuring that capital calculations are seen through the eyes of management, and reflect its thinking.

Clearly this is a challenge, even in some larger institutions that have been slow to embark on economic capital initiatives. However, it also provides an opportunity to integrate regulatory compliance into a broader and more sophisticated risk-based capital framework, capable of supporting enhanced decision-making and assuring stakeholders that the institution is robust and properly managed.

In response to the challenge, a global team at PricewaterhouseCoopers has developed a comprehensive new service offering called 'Risk-based Capital Management'[3] to assist clients to link risk and capital. Our approach supports clients from design through to detailed implementation and validation. Figure 6 describes the principal components of our service offering which is supported by detailed, practical methodologies. It also provides a useful checklist of key stages to consider in complementing risk-based capital management.

Our focus, as we are sure yours is, is about creating business benefits for our clients. There is much more to risk-based capital management than models.

Figure 6: Risk-based capital management – key stages through the process

Design	Build	Integrate	Validate
• Business case • Selection of approach, methodologies and models • Policy and framework development • Management awareness • High level programme plan/roadmap	• Risk appetite • Technical guidance • Model selection • Process design – Strategy → budgeting → performance reporting – Risk adjusted performance measures – Compensation – External communication plan • Prototype economic capital model • IT and data architecture • Capital planning • Integration plan	• Embed in management processes – Strategic planning and budgeting – Performance measurement – Data quality – Pricing – Portfolio management – Compensation – External communications • Internal communication and change management • Benefits realisation	• Business case • Selection of approach, methodologies and models • Policy and framework development • Management awareness • High level programme plan/roadmap

Source: PricewaterhouseCoopers RBCM service offer

3 'Risk-based capital management', an overview guide published by PricewaterhouseCoopers. To download a copy please visit www.pwc.com/banking

PRICEWATERHOUSECOOPERS

Securitisation – an exotic option or a necessity?

by Peter Jeffrey, Frank Serravalli, David Lukach and Michael Codling

Peter Jeffrey

Head of PricewaterhouseCoopers European Securitisation Group

Tel: 44 20 7212 5214
Email: peter.c.jeffrey@uk.pwc.com

Frank Serravalli & David Lukach

Co-Heads of PricewaterhouseCoopers US Securitisation Group

1 646 471 2669 – frank.serravalli@us.pwc.com
1 646 471 3150 – david.m.lukach@us.pwc.com

Michael Codling

Banking Leader, Australia & Head of PricewaterhouseCoopers Australian Securitisation Group

Tel: 61 8266 3034
Email: michael.codling@au.pwc.com


An expanding market

Mention 'securitisation' and one often thinks of on-off balance sheet, manipulation, Enron and Parmalat; others think of smart investment bankers, obscure language and high fees.

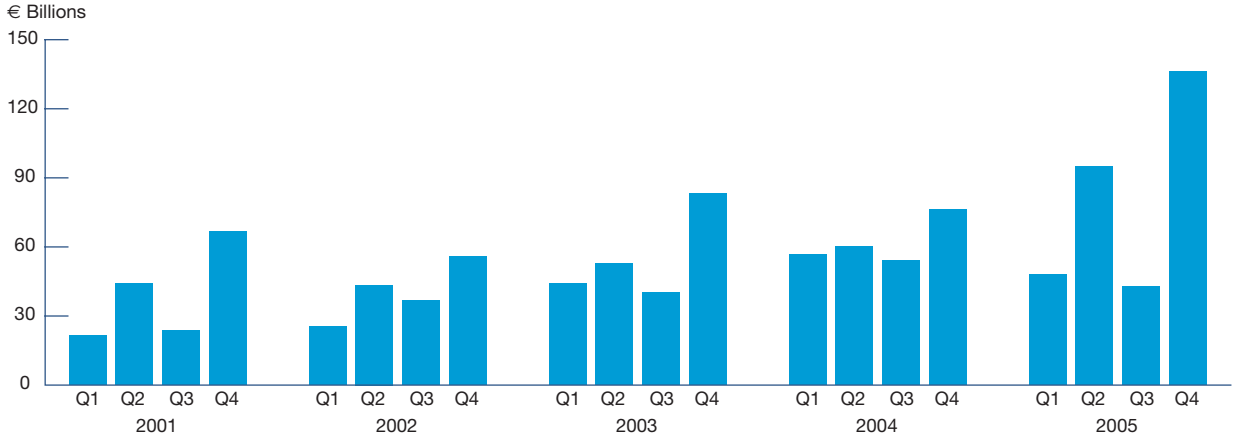
It is undoubtedly true that securitisation is complex, but equally true that it is an increasingly important tool for many companies, both within and outside the financial services sector. We believe there are also good reasons as to why this trend is set to continue, and they will be addressed later in this article.

Securitisation techniques were developed in the US in the 1980s, and has become a mature and significant sector of the capital markets. In Europe, a few securitisation transactions were undertaken in the 1980s, but it was not until the late 1990s that the market exploded. As can be seen from Figure 1 below, it has been growing ever since at an increasing rate.

In other parts of the world, Australia has a mature mortgage securitisation market and is just beginning to develop other asset classes. Japan has a domestic market, and some other Asian countries have experimented with securitisation. We have recently seen the first deals in Russia and the Middle East.

Many types of receivables and assets, that will generate future receivables, have been securitised. Some of these are listed in Figure 2.

Figure 1: European securitisation insurance



Source: Dealogic, Thornson Financial, J.P. Morgan Securities Inc., Structured Finance International-Compiled by European securitisation Forum

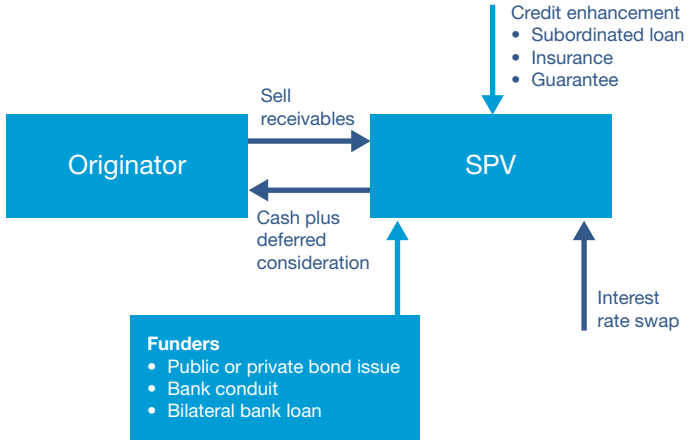
Securitisation – an exotic option or a necessity? continued

Figure 2: Securitisation issuance by asset type

Retail mortgages	Champagne and whiskey stocks
Credit cards	Pop artists back catalogue
Auto loans	Ferry and road tolls
Commercial mortgages	Account receivable
Insurance premiums	Tax receipts
Non-performing loans	Corporate loans

Source: PricewaterhouseCoopers

Figure 3: How can you use securitisation to access the capital markets?



Source: PricewaterhouseCoopers

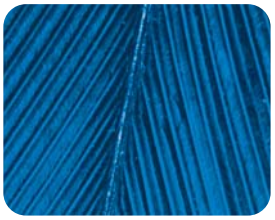
So how does securitisation work?

A company (the originator) wanting to securitise will transfer current or future receivables to a Special-Purpose Entity (SPE). This transfer needs to be what is known as a 'sale/true sale,' meaning that in the event of the originators' bankruptcy, the assets will remain the property of the SPE and will not be available to the originators' creditors.

The SPE pays for the assets by raising funds through the issuance of securities in the marketplace, either public or private. Conduits are a popular vehicle utilised to fund short-term assets. The sponsoring bank may consolidate a conduit. It is a particularly useful structure for smaller transactions and shorter-term assets.

Before arranging this funding, the SPE should consider currency and interest-rate hedges, as well as credit enhancement for the assets.

Credit enhancement means that in the event of losses, often three or four times expected losses, the originator or a third party (e.g. an insurance company) will absorb the losses.



Credit enhancement can take many forms, including a subordinated loan from the originator, credit insurance and cash reserve funds (being cash built up of cash in the SPE). This credit enhancement allows the SPE to be highly rated, thus enabling it to raise funds at highly competitive rates.

Any excess income in the SPE, after paying the funding costs, hedging costs and other expenses, is usually passed back to the originator as deferred consideration. Usually, the originator will continue to service and administer the receivables on behalf of the SPE. It is thus more attractive than an outright sale of the receivables, because it provides funding, and a limited amount of downside protection (in respect of losses incurred above the credit enhancement), while maintaining all the upside potential of the assets. It also maintains the ongoing relationships with customers, and usually, they may never know that their receivables have been securitised.

A key to making a securitisation effective is to ensure that it is 'tax neutral' as far as possible both from a direct and indirect tax perspective. In some jurisdictions, this is relatively easy whilst in others 'offshore' SPEs are required. Tax opinions will be produced to show there is no significant tax cost as a result of the securitisation.

Case study:

A Scandinavian privately owned company manages a number of retail outlets and has its own in-house store card. It is unrated, because its owners do not want to submit to the intrusive rating process. Traditionally, it has funded itself through bank loans. The rate on these were good, because of the company's track record and reputation. The company was told that in anticipation of Basel II its funding cost would rise up to 100bp. The company developed a securitisation programme for its store card receivables and obtained funding around 30bp above its historic level, thus saving 70bp.

The net result of the structuring is that the originator has raised funding whilst maintaining the right to the profit on the receivables.

So why is securitisation attractive to companies?

It enables a company to raise funding not linked to its credit rating. This enables companies to raise funds from sources that would not normally consider funding such a company. It also does not utilise existing funding lines or limits.

Because of the high credit rating of the SPE, overall funding may be reduced. This will become particularly important as banks adopt Basel II and will have higher capital changes for lending to unrated and lower rated companies.

In addition to being an effective funding technique, securitisation may provide other benefits. It may be used as a risk mitigation tool, for catastrophic risk. The originator bears the cost or pays for protection in respect of three or four times expected losses. If losses are greater than this, the note holders bear these losses. Thus, for regulated entities, it will usually reduce the regulatory capital requirement they have on the securitised assets.

Depending on your accounting programme, which will be discussed later, securitisation may result in earnings when assets are securitised.

Securitisation – an exotic option or a necessity? continued

Case study:

A US mortgage company generates value from originating mortgages through its 'state-of-the-art' IT systems and extensive broker network. The company has little interest in holding or servicing mortgages long-term. By securitising its mortgages and passing the servicing to a specialist mortgage servicing company, the mortgage company can realise funds to finance new loans and at the same time, under US GAAP, generate a gain on sale, thus realising the inherent value of the origination process.

A frequent comment from first-time issuers is that the process enables them to understand their receivables better and enhance their origination and processing systems giving them a further competitive advantage.

For companies in developing countries, where traditionally international lenders have been unwilling to lend due to the political and country risk, securitisation can be particularly beneficial. By having the SPE outside the originators country and in an established financial centre, much of the political and country risks can be removed.

Case study:

A Caribbean company with a major export business wants to raise funding for expansion. This funding cannot be sourced from the limited domestic markets, and international funders are reluctant to lend in the region. The company sets up the SPE in Delaware and sells its export receivables to the SPE. The SPE then arranges funding from a US and EURO Medium-Term Note (MTN) programme. This is possible because the funds from the receivables are kept offshore, while the MTNs are outstanding.

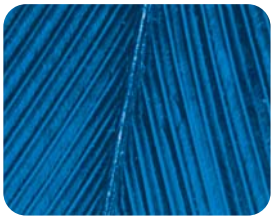
Many people associate securitisations with off-balance sheet accounting and some of the recent scandals mentioned earlier. Undertaking a securitisation purely to 'massage' the balance sheet is never a good reason for undertaking such a transaction. Equity and credit analysts are increasingly penalising companies where it is not clear why securitisations have been executed.

On the other hand, the same analysts give significant credit to companies which use securitisations in a strategic manner and can articulate the reasons for doing so. Those who combine this with good and clear financial and disclosure risks on the securitisations have nothing to fear.

In any event, in practice 'off-balance' sheet accounting is getting more difficult. US GAAP is relatively friendly to securitisations with its qualifying special purpose entity (QSPE) regime, but in recent years the FASB has tightened the rules for qualifying as a QSPE and new rules likely will be stricter.

Under IFRS, most traditional securitisations fail to achieve off-balance sheet treatment (although there is some possibility of partial derecognition) consequently, the securitised assets remain on the balance sheet with the originator bringing on to its balance sheet the funding obtained. Since no sale has taken place, no upfront income recognition is allowed.

Currently, there is an intention to converge US GAAP and IFRS, which in the case of securitisations will not be easy. The securitisation industry world-wide is currently working to develop an accounting approach that will best account for the complex economics of a securitisation. This is an initiative of the European, Australian and US securitisation forums, which have to



date, undertaken a worldwide survey of the accounting needs of securitisation and how current accounting regimes meet these needs. The results of this survey have been discussed with IASB, FASB and other regulators. We would encourage all securitisers to get involved with this initiative and to provide their ideas for the future. The authors would be pleased to receive your comments.

Accounting has, however, become less important in many parts of the world (outside the US) as regulators have developed their own rules for determining regulatory capital requirements, and this is also the approach Basel II takes.

So what do you need to do to undertake a securitisation?

The first step is to undertake a feasibility study, which would include asking the following questions:

- What strategic imperative does it solve?
- Do the likely economics make sense?
- Do we have suitable receivables;
  – that can be legally transferred?
  – that have a verifiable track record?
- Do we have systems that can segregate and manage the receivables?
- Are there any other issues or advantages to be gained?
- Will there be investor demand?
- Is there anything that will make a securitisation impossible?

Only after these key questions have been answered should you proceed to commit to investment bankers and lawyers to develop a detailed plan and structure.

Case study

An Australian bank needs to reduce its regulatory capital requirement as a result of an acquisition. It has a big credit card portfolio and wants to explore if securitisation of its credit cards will solve the problem. PricewaterhouseCoopers has been appointed to undertake a feasibility study. This study takes four weeks and concludes that a credit card securitisation is feasible, but that certain systems enhancements are required. These system enhancements have been started. together with detailed planning. PricewaterhouseCoopers has been appointed Project Manager.
To speed up the process, an initial securitisation is undertaken, using a US bank conduit with plans for a public bond land issuance as a second step.

Conclusion

Undertaking a securitisation is a complex business decision requiring many functional areas of a company and a number of external professionals. It can be achieved with good project management. While securitisation professionals have a unique language, the fundamentals can be made simplified.

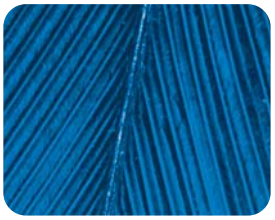
Securitisation is a technique that will become relevant and helpful to more and more companies. It can be complex to undertake, but with careful planning and project management, is achievable for most companies. In the future, we foresee it being a necessary funding technique for many companies rather than an exotic option.

It is for this reason that at PricewaterhouseCoopers we have developed a global securitisation practice, which helps clients make complex business decisions in

Securitisation – an exotic option or a necessity? continued

undertaking a securitisation as easy as possible. Our practice with major centres in the US, Europe and Australia, and we work with both the largest securitisors in the world, as well as those undertaking their first securitisations. Our global practice takes the best experience and knowledge from around the world and helps clients develop a securitisation process to enhance their businesses. The authors of this article are significant members of the various securitisation trade bodies, that continue to influence major market developments.

The global practice has written 'A Guide to Global Securitisation Transactions' and 'The Practioners Guide to Securitisation' (on behalf of City and Financial), which while written from a UK perspective, will be of value to all first-time securitisors.



PRICEWATERHOUSECOOPERS

Confident in compliance?

by Martin Hislop, Jan Willem Kaptein and Alex Shapland

Martin Hislop

Senior Manager, Risk Assurance Services, UK

Tel: 44 20 7804 1126
Email: martin.hislop@uk.pwc.com

Jan Willem Kaptein

Manager, FS Regulatory Compliance, The Netherlands

Tel: 31 10 407 6392
Email: jan.willem.kaptein@nl.pwc.com

Alex Shapland

Director, Financial Services Regulatory Practice, UK

Tel: 44 20 7213 8618
Email: alex.shapland@uk.pwc.com


Recent changes in laws and regulations, together with scrutiny of key supervisors in the US and EU are driving an increased focus on the compliance function. Boards and CEOs seeking to discharge their accountabilities[1] increasingly place compliance on their agendas. But what does it take for the organisation to respond to such scrutiny with confidence?

This responsibility falls primarily on the Head of Compliance, for whom a key obligation is to provide information regarding compliance of the business with relevant laws and regulations – a complex, and often arduous, task when the business spans several territories and regulatory jurisdictions. In turn, Heads of Compliance are seeking more assurance and a higher level of confidence about:

- How effective business processes are at managing compliance risks;
- The performance of the compliance function;
- The escalation and communication of compliance matters.

Many organisations that have identified limitations in their current compliance monitoring and reporting capabilities are now seeking to improve their compliance intelligence through new or enhanced reporting processes. This article explores what it takes to establish a leading edge compliance reporting framework that better informs the Board, challenges the compliance network and more effectively engages the business on matters of compliance.

How confident is management in understanding the:

- Impact of compliance on the organisations reputation;
- Relationships held with key regulators;
- Effectiveness of compliance systems and controls; and
- Direct costs arising from compliance-related incidents?

Benefits of an enhanced reporting framework

Effective management information enhances the governance structure by increasing the ability of key recipients to execute their duties by informing, facilitating discussion across layers of management and supporting decision making. In addition, accountabilities can be more effectively allocated and issues can be more formally addressed.

A good compliance management information (MI) framework benefits preparers (e.g. opportunity to highlight obstacles and seek support in resolving these, report achievements) and recipients (e.g. better informed decision making, confidence in understanding the business).

If risk based, rather than being driven wholly off of detailed regulatory requirements, the compliance framework can be applied effectively across many regulatory jurisdictions, while the focus of information generated is better aligned with risk-based ambitions of the business.

1 Compliance and the compliance function in banks (p. 9), Basel Committee on Banking Supervision, April 2005. (http://www.bis.org/publ/bcbs113.pdf)

Confident in compliance? continued

Defining the objectives of compliance reporting

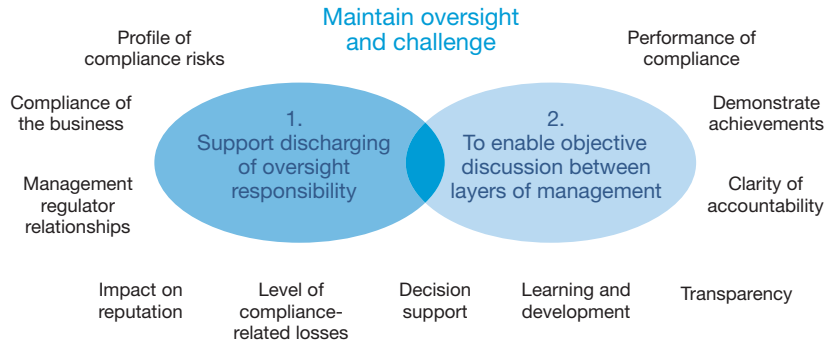
The principal purpose of compliance reporting is to allow senior management to exercise their duties in overseeing and challenging the management of compliance risks. Ideally, the same reporting structure will also support discussion and informed decision making needs at other levels of the organisation (see Figure 1).

Ultimately, compliance reporting should provide senior management with a regular and reliable view on responses to issues and incidents arising, and how these impact the:

- Current profile of compliance risk across the organisation;
- Organisation's reputation;
- Quality of relationships held with key regulators;
- Effectiveness of compliance systems and controls; and
- Costs incurred as a result of compliance related incidents.

The ability to effectively assess these matters relies on the way in which an organisation identifies, validates and reports on compliance matters that are ultimately regarded as significant at group (or regional) level.

Figure 1: Objectives of compliance reporting



Source: PricewaterhouseCoopers

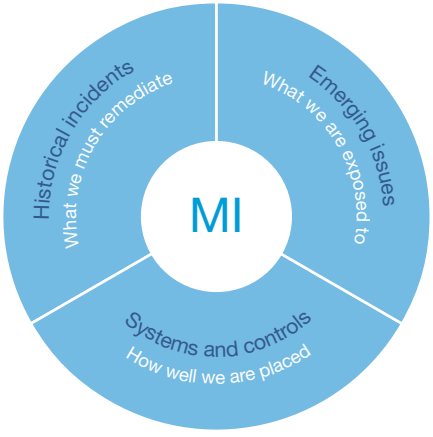
Content of management information

In order to provide recipients with information and increased confidence that compliance risks are being identified and properly managed, reports should present a picture that encapsulates what has occurred to date, but in the context of what might follow in the future. There are three key elements to consider (see Figure 2):

Historical incidents – taking ownership of and responding to incidents that crystallise is an aspect reasonably well addressed in most organisations. A view of past track record is essential to maintain support for remediation efforts and to respond to lessons learned.

Emerging issues – it is essential to know when new matters arise that impact the compliance environment, and how these are being responded to. This principally relies on the business advisory/support role of compliance, to understand what is happening within the business, and the outside world. Emerging issues may include changes in the business (e.g. new products, M&A, new territories / markets) and developments in the market (e.g. supervisory hot topics, peer organisation investigations; announcement of new regulations/directives).

Figure 2: Components of compliance information



Source: PricewaterhouseCoopers

Systems and controls – to complete the picture, and understand how well the business is placed to respond to the emerging issues, a view of the compliance control environment is necessary. A profile of residual compliance risk (from the risk assessment conducted by compliance or risk management) is invaluable, especially if reinforced with results of compliance monitoring (including monitoring conducted by the business, compliance, internal audit and the regulator as appropriate). Other matters that should be incorporated into the ongoing assessment of the control environment include: the high risk internal and external audit issues related to compliance matters, status of training provided to the business and the nature and status of requests from regulators.

The other important aspect of effective compliance reporting is measuring the performance of the compliance function. The management style of the compliance function will determine what is relevant to report in the way of performance. The principal angles to address here include:

- Annual plan and objectives: assessing the degree to which financials, compliance training plans, compliance projects are performing against target;
- Operational level agreements / internal contracts: identifying how compliance has worked with or delivered to the business against operational targets.

Data sources

The key data sources that support the enhanced compliance reporting envisioned in this article are explored below. Some are not traditionally owned or maintained by compliance, which presents challenges such as negotiating access and ensuring quality and suitability of data.

However sourced, owned or maintained, information gathered should be auditable, and therefore is dependent on adequate records being kept (whether manual, or supported by an IT solution).

Compliance managed data sources

On the basis that compliance typically carries out three broad roles, it would be expected that there is relevant data that can be accessed from the records kept within compliance, providing the core for reporting:

- Compliance risk assessment: May be conducted by the risk function but will be key in providing the overall profile of compliance risk, e.g. by business

segment and by category of risk. This orientates users of the MI report with the overall context against which specifics are reported;

- Compliance monitoring: May be conducted in part by Internal Audit, or the business, but the coverage and results will highlight exceptions. Some exceptions may be of sufficient impact, or drive themes of weakness, to report; and

- Business advice and support: The day-to-day value added role of compliance gives exposure to the changing business environment. As such, an overview of areas such as significant business changes, results of regulator visits and outcomes of business monitoring, can be obtained.

Data sources typically maintained outside of compliance

Accessing data from sources external to compliance will improve the overall context of the messages that can be reported. This can be achieved in two ways: targeting specific compliance risk areas (e.g. in terms of Key Risk Indicators) or to provide a completeness check, or corroboration, from a source 'independent' of compliance. Examples of available data are likely to include:

Identifying and targeting compliance risk:

- In-house legal: summary of litigation cases underway/resolved (responding to compliance incidents);

- Operational risk: summary of direct losses incurred (as a result of compliance incidents);

- Business: Overview of customer complaints in the context of business volumes; results of peer-to-peer control reviews (of a compliance nature); and

- External data sources such as regulators, new/data search organisations and legal and advisory firms: provide useful summaries of changing regulatory environment, such as emerging regulation and directives, current regulatory hot topics and press announcement affecting peer organisations.

Corroboration:

- Internal audit: summary of high-risk audit issues (of compliance nature);

- Operational risk: results of risk/self assessments (where compliance aspects can be segregated).

Creating information from data – Once new reporting processes are established, accessing data becomes routine.

However, an element of value added editing and formatting will be required to translate the core data into information tailored and fit for purpose. This is particularly relevant when devising the form and content suitable for high profile reports, such as to regional committees or the group board of global organisations.

Developing the compliance reporting framework

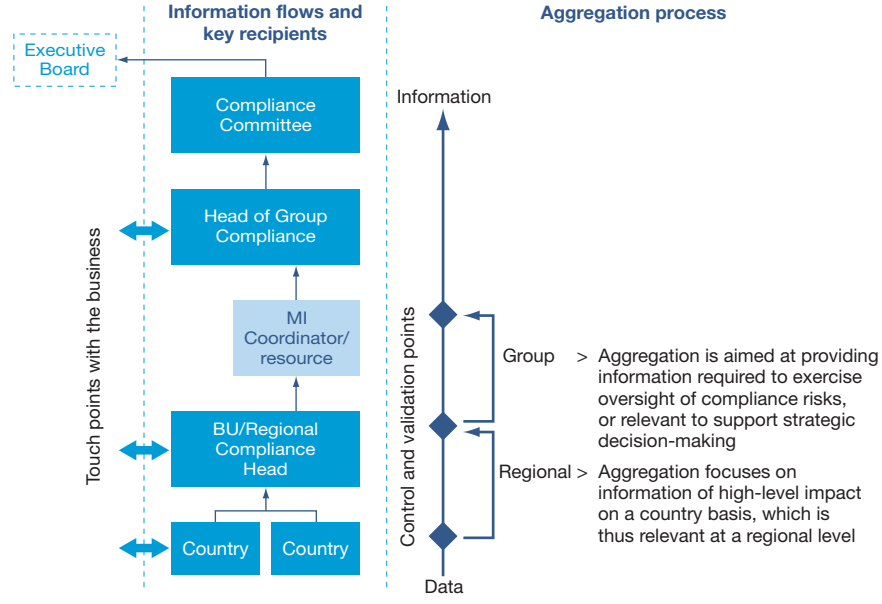
A number of key factors will determine the overarching design of the reporting framework (see Figure 3):

Recipients of information: The various stakeholders in the compliance information chain who are to receive information (Board, Sub-Committee, Head of Group Compliance, Regional Heads of Compliance) will drive the number of reports to be prepared. The purpose of these reports will drive the information that should be included, in terms of content, or level of consolidation.

Aggregation levels: Fitting the reporting framework to the organisational structure will drive out the number of aggregation levels required (country level to regional; regional to group).

Touch points with the business: Ideally, the aggregation levels will align to the key touch points that compliance has

Figure 3: Overview, management information framework



Source: PricewaterhouseCoopers

with the business (local management, business unit/divisional committees), allowing information to be consolidated to support these key business communications.

Manual or automated: The degree of automation sought in collating of data and formatting aggregated information will drive the speed of reporting and amount of effort required to maintain the reporting process. The degree of automation and available data warehousing depends on the way the reporting process is run. There is no 'one size fits all' solution to this matter, however, it is crucial that whatever approach is taken enables those who work with it to pull meaningful data in an efficient manner, while maintaining a suitable audit trail.

Supporting resources: Determining how many resources are required to support the reporting process (e.g. preparation of meaningful summaries from raw data, editing of reports to top level management) and where they should reside (centrally vs distributed) will shape where ownership sits and how the information flows reside.

Practical Challenges

In our experience, the key practical challenges to be addressed include:

Stakeholder management: Stakeholders reside at several levels of the organisation, in different business units and various geographies driving different interests.

Obtaining an organisational view: Agreeing a standard for reporting compliance in a global organisation is problematic as there are varying regulatory regimes (e.g. principle vs rules based).

Constraints in data collection: Several difficulties will be faced initially, such as sensitivity of data obtained from other parts of the organisation, limitations in the format or structure of existing data, frequency of data updates and confidence in the quality and integrity of data.

Determining what matters to report: Recipients of MI will generally be senior management, while providers of information will be at the operational level. The resulting conflicts in what is considered 'important' must be overcome to ensure information reported is relevant and informative, as well retaining efficiency.

Confident in compliance? continued

Validation and clarification: An amount of effort is required to ensure that data collected is robust. Here, keeping the process efficient and finding sources to validate are the challenge.

Presentation of information: Key reports may be visible not only to senior management, including independent directors, but they may also be made available to supervisors. Consequently, presentation should be reconsidered carefully. Encouragingly, addressing the practical challenges outlined above has usually presented an opportunity to develop or improve the relationship between compliance and the business.

So what next?

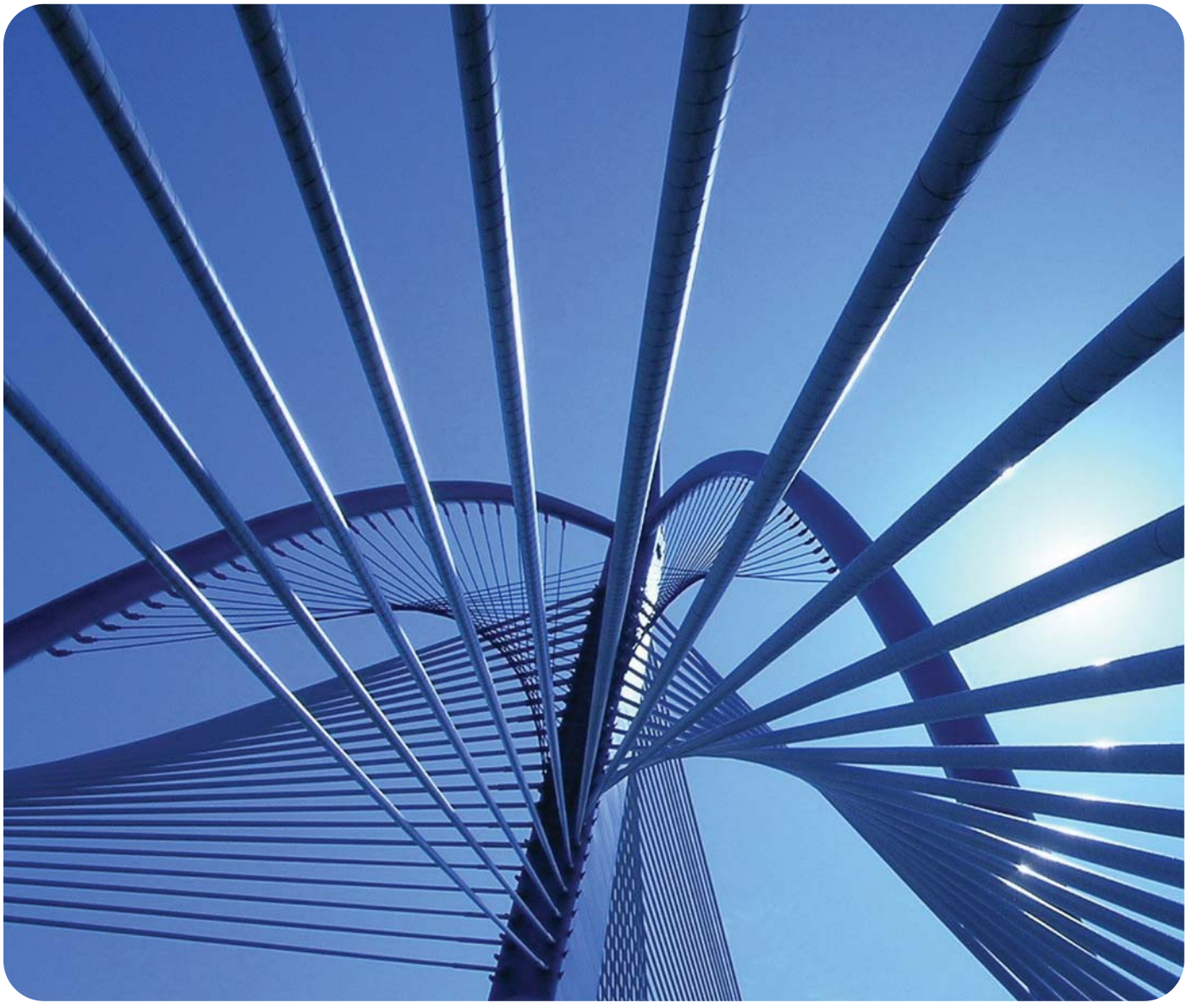
Your organisation may be one of those already engaged in creating an enhanced risk-based compliance reporting framework. If it is not, senior management would do well to consider the following questions:

- What compliance information is currently generated for the Head of Compliance?
- Is that information adequately addressing historical and emerging issues, in a high-risk based manner?
- How much of this is actually digested and used?
- What level of confidence over business compliance is gained?
- Are business management adequately challenging the awareness of and support on they get from the compliance network?
- How well do business management understand evolving compliance priorities?
- How satisfied are they that they understand and are thus able to respond to such priorities, over time, as they evolve?

PRICEWATERHOUSECOOPERS

Does identity theft affect your organisation?

by Mark Vos, Jan Schreuder and Philip Riley



Mark Vos

Director, Business Assurance, Australia

Tel: 61 8266 7739
Email: mark.vos@pwc.au.com

Jan Schreuder

Partner, Business Assurance, Australia

Tel: 61 8266 1059
Email: jan.schreuder@pwc.au.com

Philip Riley

Executive, Investigations and Forensic Services, Australia

Tel: 61 8266 3158
Email: philip.riley@pwc.au.com

Evolving threat

Reputation damage can be fatal to an organisation. Last year, a company in the United States had to close its doors, due to the reputation fallout from a single identity theft incident. Once it was reported that a number of identities were stolen from the organisation, few were prepared to do business with it as it could not be trusted to secure customer data.

The manipulation, misuse or outright theft of identity has long been part of the repertoire of criminals. The advent of information technology, particularly the Internet, has simply widened the range of opportunities for the identity thief.

The number of reported identity theft incidents has been increasing rapidly over the past few years (see Figure 1). Banks are no longer the prime target – cyber criminals are attacking an ever-broader range of institutions.

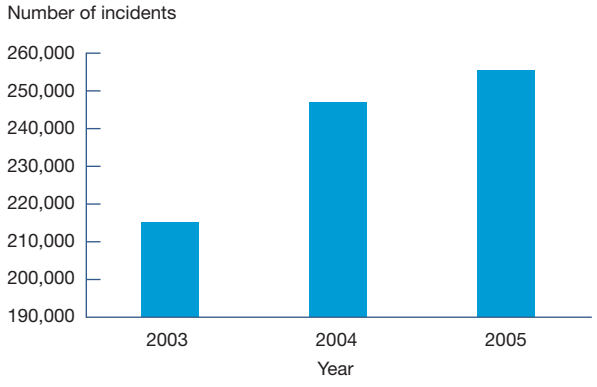
If your organisation processes and/or stores customer or personnel data, the chances are that you too are already a target for identity theft. Common identity information used to identify an individual includes driver's licence details, mother's maiden name, date of birth and home address. Also frequently used as identifiers are telephone bills and utility bills.

This information is widely collected and stored by organisations, and in turn often targeted in identity theft crimes.

Nola Watson, head of Corporate Risk Services at Insurance Australia Group, says: 'There is intrinsic value associated with identity information, whether it relates to customers or personnel. Each organisation should be aware of the identity information they store and the value associated with it, and ensure that there are adequate controls protecting it.'

Cyber criminals use a combination of orthodox methods (such as bribing a call centre staff member to physically obtain information) and electronic tools (such as keystroke loggers) to access, manipulate and exploit identity information. These range from planting individuals as staff in organisations, to launching attacks from the other side of the world via the Internet.

Figure 1: Number of reported identity theft incidents in the USA



Source: USA Federal Trade Commission – 2006

Does identity theft affect your organisation? continued

A compounding factor in the risk equation is that the range of data stolen and the risk of exposing customer information increases as functionality and product ranges are added to systems to take an organisation closer to its customer base. Examples of this are banks providing Internet banking services or airlines allowing customers to see their booked flights or their frequent flyer points online.

Against this background, organisations are asking: how much of an issue is identity theft? What is the best response? And how will it impact their business?

How much of an issue is identity theft?

Estimates of cost attributable to identity theft vary around the world, but there is no doubt that it is a serious and growing concern.

In 2003, the United States (US) Federal Trade Commission found that 215,000 reports of identity theft and fraud had cost Americans at least US$437 million. By 2005 the number of reports had risen to 255,000, representing approximately 40% of all complaints filed with that agency in 2005.

Identity theft occurs by a range of means. It might be an employee walking out of the office with photocopies of customer files. At the other end of the spectrum, it may involve cyber criminals using the Internet to gather or misuse identity information. This is a source of greater risk due to the capacity of criminals to steal vast quantities of data without geographical boundaries.

In its current state, identity theft via cyber crime is in its early stages, with networks of criminals typically exploiting customer data using orthodox criminal techniques. However, these groups are becoming more sophisticated by attacking electronic information without having to be in the physical presence of the information.

As organisations strive to aggregate customer data to provide onselling opportunities, this makes it easier for cyber criminals to steal it electronically. Once stolen, the data is then being sold in underground networks so others can assume the identity of the victim. The data may also be employed in a new range of crimes across the globe, often without the immediate knowledge of the victim as the information is stolen electronically without detection. The impact of these new crimes will be compounded by their novelty and the increasing difficulty in mitigating them.

In the PricewaterhouseCoopers (PwC) Global Economic Crime Survey 2005, 54% of companies surveyed revealed that they had suffered from economic crimes involving false pretences and money laundering, both crimes in which the manipulation of identity plays a key part.

It is interesting to note that only 22% of companies reported that they perceived false pretences and money laundering were prevalent in their business. This highlights a significant gap between the actual incidence and damage of identity theft and the actions that many companies are taking.

Findings from:
Global Economic Crime Survey 2005, PricewaterhouseCoopers and Martin Luther University, Halle, Germany, 2005.

Many experts are concerned about the ‘deferred loss of identity theft’, wherein thieves sit on stolen identities for months or years until victims believe the danger has passed. It’s hard to put figures on potential outcomes like that.

Findings from:
The State of Information Security 2005, A worldwide study by CIO magazine and PricewaterhouseCoopers.

We often read about successful identity theft attacks on organisations. The perception is that such attacks are focused on banks, but the following headlines show that the problem extends far beyond the finance sector.

'Virus-infected computer compromises personal information for about 2,500'
The Gazette, Feb 2006

'12,000 notified about names and Social Security numbers on recovered stolen computer'
Duluth News Tribune, Jan 2006

'226,000 notified about personal data on stolen laptop'
Wired News, Jan 2006

'Personal and financial information of some university donors may be at risk'
The Observer Online, Jan 2006

'Estimated 40 million credit card numbers possibly compromised'
Security Focus, Oct 2005

'Personal information for 700 patients possibly compromised'
post-gazette.com, Jan 2006

What is the best response?

Consistent and cooperative approaches to this intricate and escalating problem will assist in preparing both the community and organisations for the potential dangers.

Identity theft threatens all parties involved in Internet or electronic transactions and carries the potential to cause significant damage to groups that hold personal information online. In turn, organisations that provide trusted services on the Internet are dependent on each other for maintaining customer confidence in this new channel. For example, if a major bank was to fall victim to a successful identity theft crime via Internet banking, this could affect the entire trust model of Internet banking in the industry, not just for the bank that was victim to the crime, but for any bank providing Internet banking services.

The problem of identity theft is beyond the capacity of any one organisation to manage. Moreover, cyber crime tends to flourish when threats are treated discretely, rather than addressed through uniform, cross-industry solutions. By working together in the cause of national and international 'target-hardening', organisations can play an effective role in making the Internet a relatively unprofitable place for cyber criminals to do business.

The lack of cooperation among organisations on identity theft could also increase the risk of regulators imposing additional conditions. It is therefore appropriate for organisations, industry bodies, governments, law-enforcement agencies and the community to work together in dealing with identity theft. This might include:

- Sharing threat research about identity theft;
- Industry forums on recommended standards for dealing with identity theft;
- Community working groups that provide recommended standards for users;
- Development of industry education and awareness programs; and
- International cooperation across governments and law-enforcement agencies.

Internally, there are a number of things organisations can do. As identity theft attacks increase and become more diverse, it is important to directly align the mitigation approaches to their associated risks.

Many organisations are developing risk-based decision analysis processes to enable them to allocate security

Does identity theft affect your organisation? continued

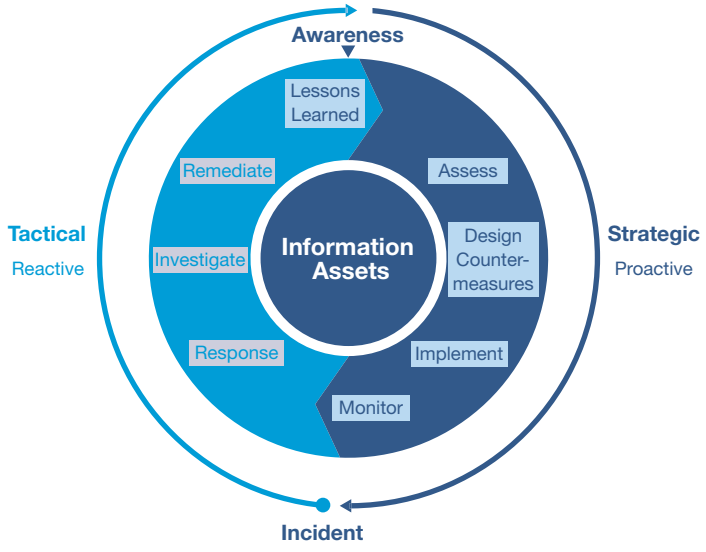
resources and prioritise security projects. A crucial component of the risk-based decision analysis is an organisation's risk and value map, which compares the expected annualised costs of security events before and after the security investment.

The risk-based decision analysis must link into an organisation's risk management life cycle. An example of the identity theft risk management life cycle is shown in Figure 2:

This process is cyclical, and never stops. From development awareness in an organisation in relation to identity theft crimes, to responding to an incident, it is important to address the risks in each phase of the life cycle, and ensure that they are understood and either accepted or addressed.

Some organisations are extending this concept further by establishing security as a separate profit centre and calculating a return on security, i.e. the return on the capital invested in security activities.

Figure 2: Identity theft risk management life cycle



Source: PricewaterhouseCoopers

To be effective, the security risk analysis processes have to be integrated with the organisation's overall risk framework. This is vital to ensure buy-in from the business, including senior management.

As organisations open up their technology systems to customers to improve services, their traditional defences are broken down. The challenge is to maintain security while moving away from traditional perimeter security models where only employees can access company data. The key to success is to establish robust data classification models, as well as strong identity management processes and systems, as this will allow an organisation to take different mitigation strategies depending on the value, criticality and sensitivity of the information within an organisation, commensurate with the risks.

The one type of technology organisations do seem to be investing in is identity management – not surprising as a reaction to the ID theft epidemic.

Findings from:
The State of Information Security 2005, A worldwide study by CIO magazine and PricewaterhouseCoopers.

Other practical measures organisations can adopt are to:

- Develop, publish, and implement a privacy policy;
- Only store essential data;
- Do not store customer data that is only required temporarily;
- Ensure call centre customer logs do not hold personal data;
- Limit employee access to data;
- Monitor employees who have access to personal data (within the parameters of privacy and workplace laws);
- Immediately report security breaches; and
- Request only customer information that is required for the transaction.

How will it impact the business?

It is critical to strike the right balance between keeping the bad guys out and not impacting the business so much that your competitive edge suffers.

In an increasingly virtual business environment where Internet-based applications are deployed by customers, employees, suppliers and other business partners, security is as much about appropriate inclusion – allowing access to the right people – as it is about prevention.

Identity theft requires a whole-of-business solution, tailored to the particular risks an organisation faces. There is little point having the most sophisticated firewall available if the business faces a greater risk from someone removing a box of files from the premises.

What can you do next?

If you have not already done so, the first step is to conduct a risk assessment to determine what identity theft risks you face. This will allow you to take a risk-based approach, ensuring a cost-effective, business-focused action plan that balances the cost of mitigating the risks against acceptance of risk. It is recommended that you use your organisation's existing risk management framework to perform this assessment, as that will provide the results in the same way as other risks to your organisation.

Once risks are determined, it is important that the business units take ownership of these, rather than assigning them to the information technology team. It should be up to the business units to make the initial assessment as to whether the risks should be accepted or mitigated, as they are the ones who own the information.

When the organisation makes a decision on how the risks are to be treated, it should be both the business units (for business processes-related issues) and the information technology team (for technology related issues) responsibility to mitigate these risks.

PRICEWATERHOUSECOOPERS

Contact details

Editor-in-chief

Chris Lucas
Chairman, Global Banking
& Capital Markets Executive Team

Tel: 44 20 7804 9652
Email: christopher.g.lucas@uk.pwc.com

Editor

Darren Meek
Partner, Banking & Capital Markets, UK

Tel: 44 20 7212 3739
Email: darren.l.meek@uk.pwc.com

The Markets in Financial Instructions Directive: European regulation with global impact

Graham O'Connell
Director, Financial Services
Regulatory Practice

Tel: 44 20 7212 3826
Email: graham.r.oconnell@uk.pwc.com

Matthew Oswald
Senior Consultant, Financial Services, UK

Tel: 44 20 7804 4230
Email: matthew.c.oswald@uk.pwc.com

Russia's banking sector: Huge growth potential for aggressive players

Rick Munn
Industry Leader, Financial Services, Russia

Tel: 7 495 967 6342
Email: rick.munn@ru.pwc.com

Evgeniy Kriventsev
Senior Manager, Financial Services, Russia

Tel: 7 495 967 6373
Email: evgeniy.kriventsev@ru.pwc.com

Oleg Mosyazh
Manager, Financial Services Marketing, Russia

Tel: 7 495 967 6074
Email: oleg.mosyazh@ru.pwc.com

The practical application of Pillar 2

Richard Barfield
Director, Valuation & Strategy, UK

Tel: 44 20 7804 6658
Email: richard.barfield@uk.pwc.com

Shyam Venkat
Partner, Advisory, Financial Risk Management, US

Tel: 1 646 471 8296
Email: shyam.venkat@us.pwc.com

Chris Matten
Partner, Banking and Capital Markets Industry Group, Singapore

Tel: 65 6236 3878
Email: chris.matten@sg.pwc.com

Securitisation – an exotic option or a necessity?

Peter Jeffrey
Head of PricewaterhouseCoopers European Securitisation Group

Tel: 44 20 7212 5214
Email: peter.c.jeffrey@uk.pwc.com

Michael Codling
Banking Leader, Australia & Head of PricewaterhouseCoopers Australian Securitisation Group

Tel: 61 8266 3034
Email: michael.codling@au.pwc.com

Frank Serravalli
Co-Head of PricewaterhouseCoopers US Securitisation Group

Tel: 1 646 471 2669
Email: frank.serravalli@us.pwc.com

David Lukach
Co-Head of PricewaterhouseCoopers US Securitisation Group

Tel: 1 646 471 3150
Email: david.m.lukach@us.pwc.com

Confident in compliance?

Martin Hislop
Senior Manager, Risk Assurance Services, UK

Tel: 44 20 7804 1126
Email: martin.hislop@uk.pwc.com

Alex Shapland
Director, Financial Services Regulatory Practice, UK

Tel: 44 207 213 8618
Email: alex.shapland@uk.pwc.com

Jan Willem Kaptein
Manager, FS Regulatory Compliance, The Netherlands

Tel: 31 10 407 6392
Email: jan.willem.kaptein@nl.pwc.com

PRICEWATERHOUSECOOPERS

Contact details continued

Does identity theft affect your organisation?

Mark Vos
Director, Business Assurance, Australia

Tel: 61 8266 7739
Email: mark.vos@au.pwc.com

Philip Riley
Executive, Investigations and Forensic Services, Australia

Tel: 61 8266 3158
Email: philip.riley@pwc.au.com

Jan Schreuder
Partner, Business Assurance, Australia

Tel: 61 8266 1059
Email: jan.schreuder@pwc.au.com

The journal is supported by the Global Banking and Capital Markets Executive Team

Chris Lucas
Chairman, Global Banking and Capital Markets Executive Team, UK

Tel: 44 20 7804 9652
Email: christopher.g.lucas@uk.pwc.com

Richard Collier

Tel: 44 20 7212 3395
Email: richard.collier@uk.pwc.com

Nigel Vooght

Tel: 44 20 7213 3960
Email: nigel.j.vooght@uk.pwc.com

Rahoul Chowdry

Tel: 61 8266 2741
Email: rahoul.chowdry@au.pwc.com

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services for public and private clients. More than 130,000 people in 148 countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders.

'PricewaterhouseCoopers' refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

The banking and capital markets journal is produced to address key issues affecting the banking and capital markets industry. If you would like any of your colleagues added to the mailing list, or if you do not wish to receive further editions, please write, fax or e-mail: Carly Taylor, PricewaterhouseCoopers, Southwark Towers, 32 London Bridge Street, London SE1 9SY. Fax number: (44) 20 7212 4152 E-mail: carly.taylor@uk.pwc.com

Designed by studioec4 18018 (06/06)

www.pwc.com