Frontiers in Finance
For decision-makers
in financial services
Summer 2014

Cyber threats in the Spanish banking sector
Page 6

Cyber crime:
Insurers in the firing line
Page 8

Frontiers
in Finance

Governance strategies for managing the data lifecycle:
Knowing when to fold versus hold and protect
Page 14

KPMG
cutting through complexity

Presentación

Ya lo decía Bob Dylan: "Los tiempos están cambiando". Como ocurre en casi todos los sectores de actividad, las entidades financieras tienen que responder a los avances rápidos y transformadores que se producen en el campo de los datos, la información y la tecnología. Son tan significativos y su alcance es tan amplio que afectan directamente a la estrategia global de las entidades tanto a la hora de generar ingresos y aumentar los beneficios, como de garantizar un cumplimiento eficaz de las demandas de los reguladores, que son cada vez más complejas.

Esta importancia fundamental acarrea riesgos y exigencias para que la gestión sea eficaz, pero también ofrece importantes ventajas en cuanto a eficiencia, rentabilidad, relaciones con clientes y propuestas de valor para estos. En este escenario, la función que desempeña el máximo responsable de tecnologías de la información (CIO, por sus siglas en inglés) nunca ha sido tan importante como ahora para el éxito futuro de la entidad.

Sacar partido de las nuevas tecnologías y de la gestión de datos exige aplicar enfoques novedosos a sistemas, procesos y gobierno corporativo. Mejorar la coherencia entre los datos y los sistemas de información en los que se basa la dirección interna y los reguladores externos es fundamental. Creemos que los artículos de este número contribuirán a arrojar luz sobre algunas orientaciones para el desarrollo futuro.

Entre los textos de esta edición de Frontiers in Finance incluimos uno de Marc Martínez, socio responsable IT Advisory Risk Consulting de KPMG en Madrid, en el que se analizan las implicaciones de las ciberamenazas en la industria bancaria y cómo se materializan. Según diversos estudios, España es el segundo país que sufre un mayor número de ciberataques bancarios, por lo que es un objetivo prioritario para el sector financiero la lucha contra este tipo de fraude.

Algunas de las principales compañías del sector en España ya se han puesto en marcha para rediseñar su estrategia de ciberseguridad con el objetivo de incorporar medidas de detección y prevención tempranas. El fin último es que el impacto de los posibles ciberataques se vea reducido al mínimo.

Pero en la medida en que los bancos se han vuelto más sofisticados y efectivos a la hora de defenderse frente a los ataques, el foco del cibercrimen está cambiando. En el artículo *Cyber crime: insurers in the firing line* se deja constancia de cómo las compañías aseguradoras se están convirtiendo en el objetivo. El riesgo es real y serio, por lo que las aseguradoras tienen que posicionarse rápidamente. Asimismo, este número recoge las conclusiones de una mesa redonda sobre regulación, en la que expertos de KPMG muestran el creciente interés de los reguladores por los datos y la tecnología y sus implicaciones.

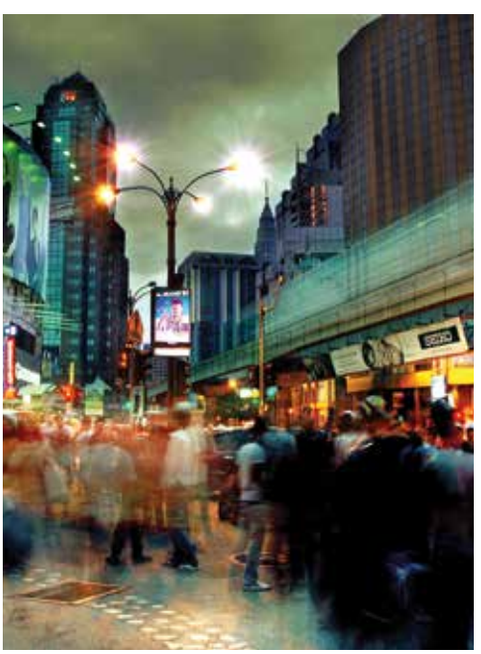
Por otro lado, hay una enorme actividad en el momento actual en el sector de pagos, impulsada por los avances en las comunicaciones y la tecnología asociada. Por ello, el artículo *Technology and payments: Beyond the hype?* se ocupa de cómo las empresas de servicios financieros, las de pagos y los nuevos operadores están haciendo grandes inversiones y lanzando nuevas iniciativas innovadoras y compitiendo por el liderazgo en lo que es un mercado en constante transformación.

El resto de artículos de este número de *Frontiers in Finance* se centran, entre otros temas, en la importancia de alinear el *reporting* de los bancos con la consecución de valor para el accionista y de las estrategias para la gestión del ciclo de vida de los datos en las firmas de servicios financieros.

Francisco Uría
Socio responsable del Sector Financiero de KPMG en España

CONTENTS

FEATURES



PUBLICATIONS

Jeremy Anderson
Chairman Global Financial Services

Data, analytics and technology: Core strategic enablers

Jeremy Anderson
Chairman Global Financial Services

Financial institutions are increasingly reliant on data and information technology as the foundation of efficient operation, regulatory compliance and future growth and profitability. This pervasive data reliance carries risks as well as opportunities. The role of the chief information officer (CIO) in helping navigate a path through this complexity is now fundamental to institutional health and integrity.

It is hard to think of a time when the role of the CIO has been more important to the current and future health of a major financial institution. In both offensive and defensive strategy – driving revenue and earnings growth and ensuring secure and effective compliance – the contribution of the CIO and his or her team is increasingly crucial.

Across the board

The role of data and information is now integral across the business, from back-office to marketing and sales and from risk management to meeting stakeholder and regulators' expectations

- **Cost and efficiency:** It is very clear that banks' balance sheets are being completely reshaped by the major new regulatory initiatives which have followed in the wake of the financial crisis. In some cases, these are driving return on equity below the cost of capital. As a result, and in order to return to generating sustainable returns and acceptable levels of organic capital, banks have no alternative but to become leaner, simpler and more cost-effective in their operations. As a key enabler of process and workflow efficiencies, technology has a huge role to play here.
- **Exploiting data:** Mastering the massive increase in data flow and extracting the greatest value from it is fundamental to organizational health and success. The implications extend across the business operating model. At the front end, financial services firms face real challenges in managing and making sense of the vast array of information which can now be made available about the attitudes, behaviour and needs of clients, prospects and targets. Technologies such as data mining and data analytics are increasingly important as a foundation for effective marketing, sales and cross-selling.
- **Managing risk:** The financial crisis and the wide-ranging regulatory response have placed increased emphasis on the need for effective management of risk in all contexts: reputational risk, operating risk, regulatory risk. Companies now face the twin challenges of sustaining improved risk management and furnishing evidence of its effectiveness to stakeholders: regulators, clients, shareholders. Collecting, analyzing and presenting the relevant data is now indispensable to creating the foundation for strong stakeholder relationships.
- **Customer relationships:** Information technology and data management are fundamental to maintaining stable

and responsive relationships with clients who are increasingly expecting continuous access to their financial service providers on a range of online and mobile platforms. Integrating the different interface technologies and grounding them on consistent, high-quality data are essential elements in creating fast, agile communications and decision-making. Consumers do not want complexity, delays or inconsistency. Companies that cannot implement the necessary systems quickly enough will find themselves squeezed out and facing further disintermediation by technical innovators, new entrants and new technologies, like we are seeing in payments or money transfer.

- **Day-to-day operations:** Fundamentally, optimizing day-to-day operations means maximizing the use of scarce resources and ensuring that people have the right information to make optimal decisions at the right time. This requires accurate and consistent data, which can serve both to underpin the operational health of the company and satisfy internal and external requirements.

The universal importance of good data and information management across the business operating model places a huge premium on the ability to collect, aggregate and analyze data to create a 'single view of the truth': one complete and internally consistent data and information resource which can satisfy all needs. Regulators are increasingly focusing on risk data aggregation, such as in the Basel Committee's recent recommendations.[1] Whether it is a question of customer-facing operations, internal systems and procedures or external reporting, the winners will be those who can bring together data in a coherent way to serve these multiple needs most effectively.

Safeguarding the institution

The exponential increase in the volume of data necessary to the operation of financial services companies, together with institutions' increasingly critical reliance on it, carry major dangers of their own. Companies are more and more vulnerable to the loss or corruption of mission critical data and at greater risk of reputational damage and regulatory sanction if they misuse it. Data and cyber security has to move from being a peripheral and technical specialism to a central strategic concern. Proper data security has to become as much a matter of business-as-usual as securing safes or locking filing cabinets.

Similarly, when internal processes, business-to-business communication and delivery of customer services all depend so critically on data and information technology (IT) infrastructure, maintaining its integrity is a key requirement in sustaining institutional security. We see only too frequently that when critical technology, such as a payments systems, fail, even for a few hours, the impact can be widespread and immensely disruptive. Leaks and loss of sensitive customer data breach the trust between institution and client and can carry significant financial penalties. Significant reputational damage can occur if these situations are not well handled.

As systems become more global and more interdependent, they begin to resemble the organizational and contractual connectedness which contributed so much to the creation of the financial crisis. It may not be too fanciful to think that the next major crisis may arise from IT vulnerability unless defensive measures are continuously upgraded.

Here, where solutions often depend on major expenditure on IT and systems, it can be hard to quantify the need and demonstrate desired returns on capital. In a low-margin, high-complexity environment, the desirable risk-reward balance may not be immediately apparent. Nevertheless, investment to improve data security, reduce complexity and enhance the customer proposition are crucial if companies are not to be outflanked by braver or more farsighted competitors.

Seizing the benefits

It is not all danger and defensiveness. The new technologies are the way of the future and if properly developed promise major improvements in internal efficiency, external reporting and, perhaps most significantly, customer relations and customer propositions. Whether it is further development of internet and mobile channels or innovative new technologies for payments, there are major potential benefits as well as risks. The role of the CIO is now to help define an institution's core strategy against this rapidly developing background and guide investment decision-making on the basis of a clear view of risk and reward.

Technology, data and information management have been a core part of financial services for many years. They have just become more important still. Boards and executive management need to ensure they are accorded the same priority as any other critical success factor.

"The universal importance of good data and information management across the business operating model places a huge premium on the ability to collect, aggregate and analyze data to create a 'single view of the truth': one complete and internally consistent data and information resource which can satisfy all needs.

1 BCBS 239, *Principles for effective risk data aggregation and risk reporting*, BIS 2013.

A leading example

One of the leaders in the new data management environment is the Commonwealth Bank of Australia. In 2012, the bank introduced a new technology platform to enable what it calls 'real-time banking' making the customer experience faster, easier and more secure. The bank's CIO, Michael Harte, explained: "What people want [whether] at home or in the office or traveling overseas, anytime, anywhere [is to have] real-time richness and be able to increasingly do that through an interface that's rich and mimics or re-presents the intimacy of what you once had [with] face-to-face banking and insurance and brokerage."[2]

These investments paid off to the extent that the bank is now introducing a range of new functions and improvements building on new technology and near field communication (NFC) payment solutions. Harte commented: "We continue to invest in rich content and the back-end technology that enables us to deliver real-time value to our customers. Our strong platformance and security layers are at the heart of all our technology and have spearheaded the growth in consumer confidence in mobile banking services."[3]

2 *CommBank CIO: Future of banking is real-time, personal*, 24 August 2012.
3 *CommBank extends lead in mobile banking and payments space*, 17 October 2013, https://www.commbank.com.au/about-us/news/media-releases/2013/commbank-extends-lead-in-mobile-banking-and-payments-space.html.

Cyber threats in the Spanish banking sector

Marc Martínez, KPMG en España

Computer crime – cyber crime – is one of the fastest growing areas of criminal activity today. The steady digitalization of business processes and the rise in the use of mobile devices contributes to the exponential advance in the types of threat and the sophistication of cyber crime.

Cyber criminals take advantage of the speed, ease and anonymity afforded by technology to undertake a wide range of criminal activities. Furthermore, the global nature of the internet has allowed criminals to embark on all kinds of illegal activity in every part of the world, so it is essential for all countries to adapt their internal control and security measures in order to address not only traditional crime but also the new crimes perpetrated in cyberspace.

Implications of cyber threats to the banking industry

In recent years, cyber attacks have become a significant threat for financial institutions and the financial system as a whole. The emergence of this type of threat at various different levels is due to the explosion of online banking together with the growing willingness of consumers to divulge personal information through the internet. The implications of the new cyber threats are very varied:

- *Financial and reputational damage:* an increased risk of loss of sensitive information (including intellectual property and confidential corporate data), which can give rise to fines or sanctions. On the other hand, an entity's image and reputation can also be undermined by a loss of trust in its online transactions, which would also lead to financial losses.

Contact
Marc Martínez

- *Global threat:* given the interconnectivity of banks and financial institutions, an attack on one bank can leave other financial institutions vulnerable to interruption, posing a threat to the security and stability of the financial system as a whole.
- *Increased information technology (IT) budget allocation:* the onset of new cyber threats and cyber risks means that banks must reassess their IT budgets to tighten their security measures, installing and implementing anti-virus software, perimeter security measures and devices, safety mechanisms and, in general, maintaining security standards and policies adapted to the new and shifting threats.
- *Interruption of business:* a cyber attack can inflict serious damage on business operations, databases and communications, translating into financial loss, reputational risk and legal damage.

What form can these threats take?

The financial sector's current strategy for protecting itself from cyber threats pivots mainly on prevention and detection, as these are under the constant scrutiny of regulators and customers. It is also important to adequately address the need to manage and protect information appropriately, and to have rapid response and recovery capacities in place, should the need for them arise. Some of the main cyber threats that pose a risk to the financial sector are:

- *Access to bank accounts.* Some cyber criminals obtain access to online banking customers' bank accounts through phishing (fraudulent techniques used to obtain confidential client information such as account numbers, passwords, etc.). Attacks carried out using such information are most frequently used for fraudulent money transfers and credit card fraud.
- *Payment service providers. Cyber criminals* launch attacks to hack the networks of payment service providers and obtain personal customer data for subsequent use.
- *Mobile devices.* Cyber criminals may gain access to users' credentials and account information by installing malware on mobile devices (tablets, cellular phones, etc).
- *Manipulation of ATMs.* Card readers can be installed at ATMs, both inside or out, to fraudulently obtain card numbers and PINs. Once this information has been obtained, it can be sold or else used to issue false credit cards with which to withdraw funds.
- *Supply chain infiltration.* Cyber criminals launch attacks on suppliers of financial institutions, including technology, software and hardware vendors. Subsequently, when a financial institution installs the infected equipment or software, its security is jeopardized.

In summary, viruses and worms, spam, Trojan horses, identity theft, denial of service (DoS) attacks, advanced persistent threats (APTs), malware, scareware, phishing, tax fraud and credit card theft are some of the real threats faced by financial institutions on a day-to-day basis.

It is imperative for financial institutions to be able to identify the potential risks that concern them and thereby confront the new threats to cyber security. Ideally, it would be advisable for them to develop a common framework based on key risk and performance indicators through which to gain a precise understanding of the scope of cyber threats.

Cyber security in Spain

National economies depend to a great extent on their IT systems and technological infrastructure. Consequently, the stability and future of these will be linked in part to the security of cyberspace in the country in question.

To that end, last February the Spanish government set up the National Cyber Security Council, formed by a panel of experts on IT security. Furthermore, a National Cyber Security Strategy has been defined to serve as a framework for both the financial sector and any other sectors subject to potential cyber attack.

Lastly, it should be highlighted that according to several studies carried out, Spain ranks second in the list of countries where cyber attacks are launched on banks, so the fight against fraud has become a top priority for the financial sector.

Some of the main Spanish financial sector firms have already begun to redesign their cyber security strategy in order to build early detection and prevention measures into their processes and bolster their response and recovery capacity to the greatest extent possible and minimize the impact of potential cyber attacks.

> The financial sector's current strategy for protecting itself from cyber threats pivots mainly on prevention and detection, as these are under the constant scrutiny of regulators and customers. It is also important to adequately address the need to manage and protect information appropriately, and to have rapid response and recovery capacities in place, should the need for them arise.

MORE INFORMATION
Marc Martínez
Socio responsable de IT Advisory Risk Consulting en Madrid
KPMG en España
T: +34 91 456 59 74
E: marcmartinez@kpmg.es

Contacts (from left)
Stephen Bonner
Jon Dowie
Kevvie Fowler



Cyber crime: Insurers in the firing line

Stephen Bonner, KPMG in the UK
Jon Dowie, KPMG in the UK
Kevvie Fowler, KPMG in Canada

As banks become more sophisticated and effective at defending themselves against attack, the focus of much cyber crime is changing. Increasingly, insurance companies are becoming the target. The risks are very real and very serious. Insurers need to raise their game as a matter of urgency.

The focus changes

When asked exactly why he robbed banks, the infamous American criminal Willie Sutton is alleged to have replied, not unreasonably, "Because that's where the money is." In more recent years, with the massive growth of the internet, online connectivity and remote access, it has again been banks which have borne the brunt of cyber crime. Not only is the money there; banks also hold critical information about all of their customers which, in the wrong hands, can be equally valuable. However, the focus of much cyber crime is now changing rapidly, away from banks and onto insurers.

There are a number of reasons. Perhaps the most significant and straightforward is simply that over the last 10 years or so, banks' defenses have become more sophisticated and effective. The industry has appreciated the threat and has taken measures to counteract it. Key steps have included implementing layers of technical protection as well as concerting efforts across the industry – in what is, after all, a challenge facing all banks – to exchange information and develop strong counter-measures together. It is clearly not possible to prevent all attacks from succeeding and for obvious reasons, individual banks are reluctant to publicize those attempts which do result in loss. But overall, the banks have become increasingly effective in repelling cyber crime.

Another key factor is that cyber criminals have come to realize that banks are not the only potentially lucrative targets. Certainly, banks are where the money is. But money can also be stolen from insurance companies. Furthermore, money is not the only valuable commodity available; insurers need to protect premium rating tables, claims and accident and loss information. Almost equally valuable are customer details – personal information, names, addresses, account details, passwords, health and lifestyle information, payment card information, etc. – which can either be parlayed into cash or sold on to other criminal interests that will attempt the same thing.

In addition, insurers typically enjoy far less close and frequent interactions with their clients than banks. Despite the hollowing out of the bank-client relationship in recent years, it is still true that banks and their clients typically transact business many times a week or month. By contrast, insurers may interact with their clients only when there is a claim or, in the case of life companies, when the client retires or dies. This remoteness from the client means that insurers are much less well-placed to identify potentially fraudulent or criminal attacks. And although attempts at insurance crime may still be less common that bank crime, the rewards for success can be much greater. Compromising a bank card or credit card may yield a few hundred dollars; a successful fraudulent insurance claim may produce an order of magnitude more. Nor is simple financial advantage the only motivation. As we shall see, insurers, along with many other financial services companies, face multiple challenges.

As insurers amass greater amounts of customer data through new online channels, social media, telematics and web-based claims management systems, they become even more attractive to cyber criminals. In 2012, a major security breach of a US insurer affected 1.1 million policyholders and potential customers. Hackers stole names, social security numbers, driver's license numbers and dates of birth. The insurer acted swiftly, offering credit monitoring and identity theft protection for those impacted, including US$1 million in free identity theft insurance coverage with no deductible. In another case, a global insurer was fined £2.2 million for failing to have adequate systems and controls in place to prevent the loss of customers' personal information.

Understanding the threat

In order to understand – and protect against – the threat, it is important to understand the range of sources.

- **Organized crime:** It may be tempting to think that the threat from cyber crime is relatively limited and arises from opportunistic attempts to extract small amounts of benefit. But experience over recent years has demonstrated conclusively that highly advanced organized crime syndicates are increasingly determined in their attacks on financial services companies and, recently, insurers in particular. These are sophisticated and ruthless criminals. Their tools of choice include malware and botnets that install themselves on corporate networks, either compromising security and transmitting critical data outside the company or transforming local networks into 'slaves' under the control of the external criminals.

  Organized criminal networks have also begun to realize that it is not actually necessary to steal anything. The mere threat of loss – or of operational damage and disruption – can be enough to extract a substantial ransom from the targeted organization. Once again, many companies are reluctant to reveal publicly when they have been hit. But many have paid up quietly.

  Reverse engineering of the malware distributed by cyber criminal organizations can reveal the kind of targets crime networks are focused on; increasingly over the last year or so, the evidence is that insurance companies are becoming targets.

  The rapid growth of online insurance purchasing offers greater opportunities to organized crime. It can be difficult for customers, attracted by low prices, to distinguish legitimate insurers from fraudulent ones. We are seeing a spate of 'ghost brokers' being set up on the internet selling fake policies, taking premiums and leaving the 'policyholder' without coverage.
- **Petty criminals:** As the term suggests, petty criminals will target any and every opportunity to compromise security and extract reward. They are comparatively indiscriminate, both in their targets and in their methodology and often are just looking for front-door vulnerabilities, such as systems with missing patches and mis-configurations that can be easily exploited. There is a modernization trend within the insurance industry currently and many insurance providers are launching portals that enable clients to self-manage their policies. Petty criminals are aware of this and are able to scan these portals using special software to detect vulnerabilities for exploitation. Ensuring front-door vulnerabilities are not present on these systems is an easy way to force the criminals to move on to the next target. Although the quantum of risk may be less than is implicated in organized crime, the threat – and the disruption which it can cause even if unsuccessful – can be significant.
- **State sponsored cyber crime:** There is no doubt that certain states have developed, and maintain, sophisticated technological capabilities designed either to extract cash or data from vulnerable Western companies or, more commonly, to sustain the capability to hold those organizations to ransom as part of a more extensive coordinated attack.

  There are fuzzy lines between traditional electronic espionage, commercial espionage and theft of data for commercial and strategic advantage. There is evidence of states engaging in commercial espionage during cross-border mergers and acquisitions (M&A) transactions. Insurance companies – along with many other industrial sectors in the West – are vulnerable to all of these dangers.
- **'Hacktivists' and terrorists:** Illegal extraction of money or data is not the only objective which motivates cyber criminals. So-called 'hacktivists', terrorists and others may be driven by a wide variety of motives, including, in particular, the desire to disrupt,

damage or destroy companies' operating capabilities. Here the threat is all the more difficult to anticipate because it can be almost impossible to predict. However, we have seen that indirect action can be especially attractive to many of the types of groups involved in these activities. For example, insurance companies that undertake business with drug companies, animal testing laboratories, defense companies and the like may well find themselves the target of cyber crime attacks from this direction.

How to respond?

The first priority is, obviously, to recognize the nature of the contemporary threat. Historically, insurance companies have sought to defend themselves against fraudulent claims by mobilizing resources to analyze broad patterns of incidence and investigate individual instances of particular concern. But the threat today includes not only the risk of financial loss, but also that of disruption to systems and processes that can cause both financial and reputational damage. The Canadian Office of the Superintendent of Financial Institutions (OSFI) recently released guidance on how financial services institutions can self-assess their level of preparedness for, and protection against, cyber attacks.[1] Insurers can also learn from the banking sector's success in creating structures and processes to share information about threats and best practices.

Second, it is a truism that insurers' back-office technology and systems are a generation or more behind those routinely employed by banks. There is a lack of connectivity and coordination between different systems and, therefore, less capability to identify and counter attempts at penetration and diversion. Less automation, more manual interventions and more breaks in the chain of information processing increase the potential vulnerability. Where claims processing is outsourced, security can be more difficult to monitor; more effective supply-chain management is needed. Recent research by Proofpoint Inc. shows that insurance companies currently face a higher number of email-based threats to security than any other business sector.[2] In fact, KPMG's 2012 *Data Loss Barometer* states that the insurance sector states is at greatest risk from social engineering attacks and system and/or human error incidents. A separate KPMG research shows that financial services companies are among those industries with the most vulnerable software.[3] Upgrading systems, although expensive, is a necessity.

Finally, and perhaps most importantly, insurers need to understand how to develop a mature and effective response. The threat is all too real. But it needs to be countered with intelligent and sophisticated action. This needs to look beyond pure technical preparedness against cyber attacks to take a rounded view of people, process and technology in order to understand areas of vulnerability, identify and prioritize areas for remediation and demonstrate both corporate and operational compliance, turning information risk to business advantage. In our experience, this means acting on six key dimensions that together provide a comprehensive and in-depth view of an organization's cyber maturity:[4]

Leadership and governance
Board demonstrating due diligence, ownership and effective management of risk.

Information risk management
The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.

Operations and technology
The level of control measures implemented to address identified risks and minimize the impact of compromise.

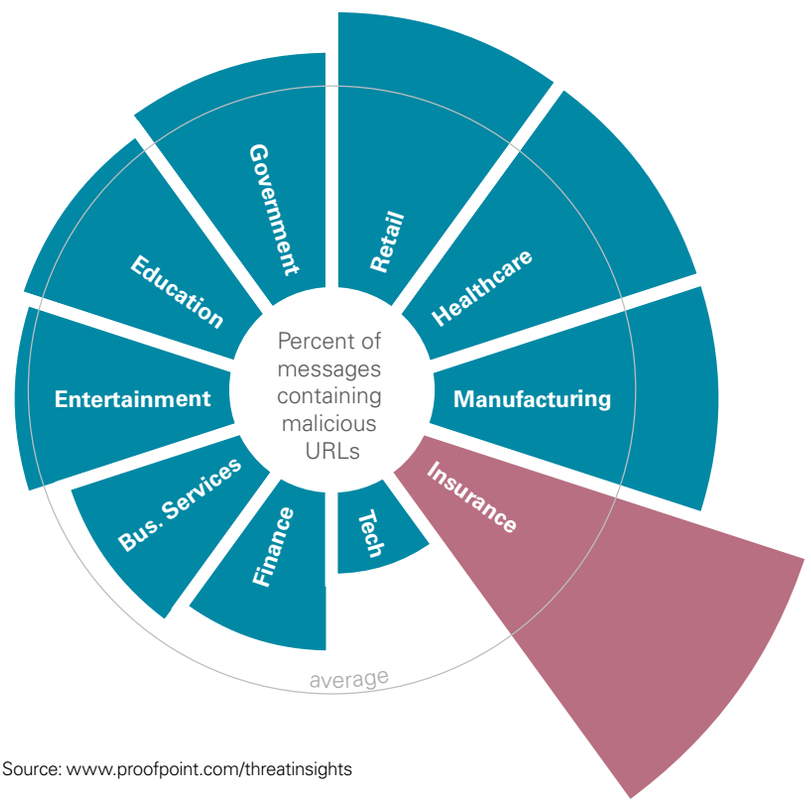
Human factors
The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge.

Business continuity and crisis management
Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder management.

Legal and compliance
Regulatory and international certification standards as relevant.

The banking sector has shown that the threat from cyber crime can be contained and countered. Insurers need to raise their game urgently to ensure that they can mount comparable defenses.

The insurance industry faces a higher number of email-based threats



Source: www.proofpoint.com/threatinsights

1 *Cyber Security Self-Assessment Guidance,* OSFI Canada, 28 October 2013. http://www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf.
2 Proofpoint Threat Insight: *Are You Being Targeted,* Part I: Industry, Poofpoint Inc. http://www.proofpoint.com/threatinsight/posts/are-you-being-targeted-part-1-industry.php
3 KPMG, *UK Cyber Vulnerability Index 2013.*
4 KPMG's Cyber Maturity Assessment (CMA) provides an in-depth review of an organization's ability to protect its information assets and its preparedness against cyber attack. cf KPMG Cyber Maturity Assessment: The cyber threat to your business, May 2013.

MORE INFORMATION

Stephen Bonner
KPMG in the UK
T: +44 20 7694 1644
E: stephen.bonner@kpmg.co.uk

Jon Dowie
KPMG in the UK
T: +44 20 7311 5295
E: jdowie@kpmg.com

Kevvie Fowler
KPMG in Canada
T: +1 416 777 3742
E: kevviefowler@kpmg.ca

Regulatory roundtable: Data and the CIO under the microscope

Giles Williams, KPMG in the UK
Pam Martin, KPMG in the US
Simon Topping, KPMG in China

In our recurring feature, experts from KPMG's regulatory centers of excellence review current developments. Here, they explore the emerging focus on data and technology and its implications.

Technology as a source of risk

Over the last 10-15 years, banks' reliance on technology has undergone a number of changes of emphasis. Initially, technology was used to streamline and automate internal back-office processes and make them more cost-effective. Then, technology gradually began to contribute to decision-making to automate various front-line processes and to create new opportunities ranging from internet banking to algorithmic trading. Now, information technology is widely used to mediate relationships with customers and counterparties and to communicate instantly and across the globe.

The consequence of such extensive reliance on technology is that weaknesses in systems and processes have become potentially much more serious, with more profound impacts. In individual institutions, failures can damage confidence and threaten brand value. When they lead to widespread contagion, systemic disruption threatens. Reliance on technology brings its own risks, as seen most vividly when systems crash (the malfunctioning or non-functioning of a major bank's automated teller machine (ATM) network is both a massive inconvenience to its customers and often a major news story) or generate instability (some sharp movements in stock prices have been attributed to flash trading and to automated and algorithmic trading more generally).

The dangers are magnified when increasing corporate and operational complexity means that few, if any, managers are any longer in a position to exercise judgment over the totality of business operations. So does the potential for systemic errors to be introduced and not be recognized. Technology risk has become a major component of operational risk and is a growing focus of concern for senior management and regulators alike.

There has been a significant regulatory focus on technology risk for decades. For example, the US Federal Financial Institutions Examination Council (FFIEC) was created in the 1970s to prescribe principles, standards and reporting formats for the federal examination of financial institutions, including their risk management systems and risk data infrastructures, with a strong focus on technology risk management. Basel II required that banks begin to hold capital against operational risk – which includes technology risk – as a buffer against the impact of operational failures. However, quantifying this risk has proven difficult. Most banks have relied on simpler standardized approaches rather than trying to construct models to calculate how much capital they should hold against operational risk.

Historically, IT risk has tended to be managed in the chief technology officer's silo (and within that, often in a sub-silo such as cyber security). In recent times, the focus has been redirected to taking data risk out of its silos and integrating it into an enterprise-wide risk management framework. Operational risk (including IT risk) must truly become the 'third leg' of the risk stool alongside credit risk and market risk. As a result, it is now increasingly understood that IT risk is too important to be left solely to IT people. The CIO has first to be an information technologist. But the CIO also has a key role to play in

Contacts (from left)
Giles Williams
Pam Martin
Simon Topping



> Risk management is intimately dependent on issues of data: data integrity, completeness, relevance and accuracy. And even in the smallest banks, good risk management depends on the IT architecture and systems used to store and process data.

informing the risk assessments of the chief risk officer. It is also important that the business line be an integral part of any technology related project, as they are ultimately the end user.

Accordingly, regulators are increasingly examining how technology risk is being incorporated into a bank's overall risk management framework.

The role of data and technology in risk management

Risk management is intimately dependent on issues of data: data integrity, completeness, relevance and accuracy. And even in the smallest banks, good risk management depends on the IT architecture and systems used to store and process data. But the many banks with multiple aging IT systems or poorly integrated inherited systems from acquisitions or mergers find it very difficult to aggregate and report data to support risk management.

The shortcomings of current practice were harshly exposed by the financial crisis. A key lesson was that large parts of the financial services industry in the US and Europe was unable to identify and aggregate risk across the financial system and to quantify its potential impact. Exposures could not be easily be aggregated across trading and bank books, across geographies and across legal entities. Risk management, governance and the underlying data infrastructure were unacceptably weak. Global systemic risk was, as a result, both obscure and under estimated.

More than 6 years after the crisis, many of these weaknesses remain. The Basel Committee published at the end of last year the results of a self-assessment by 30 global systematically important banks (G-SIBs) of their progress in meeting the committee's *principles for effective risk data aggregation and risk reporting*. The results show the lowest reported compliance rates for data architecture and IT infrastructure, the accuracy and integrity of data and the ability of banks to adapt to changing demands for data analysis and reporting. Nearly half of the banks reported material non-compliance on these principles and that they are having to resort to extensive manual workarounds. One-third of the banks reported that they will be unable to comply fully with the principles by the 2016 deadline. A report of the Senior Supervisors Group in January 2014 on data quality and management in 19 major US, Canadian and European banks reached the even more damning conclusion that:

> "...firms' progress towards consistent, timely and accurate reporting of top counterparty exposures fails to meet supervisory expectations as well as industry self-identified best practices."

Weaknesses in systems and data management have also hampered the ability of both banks and their supervisors to run stress and scenario tests. The experience of stress-testing has revealed the fact that systems and processes for aggregating and analyzing risk in large banks remain disturbingly inadequate. Ad hoc processes and manual intervention are still necessary to produce a summary of potential risks. In turn, poor or non-existent data management infrastructure casts doubt on the reliability of the assessments that are produced. There is a long way to go before the industry can convince regulators that it has the quality of data necessary to satisfy their requirements.

Responses

Many banks appreciate the need for remedial action, but are understandably wary of the scale of the task. They face competing demands for expenditure on IT and data systems at a time when they are looking to cut costs, not least to offset the increasing costs of regulation and compliance.

Supervisors are increasingly stressing the need for improvement and, at least for systemically important banks, supervisors have already increased the intensity of their supervision in areas such as banks' IT systems and data management. The question then becomes what actions supervisors are likely to take to drive improvement. This varies across countries, but in most countries, the supervisory toolkit will include the ability to require banks to take remedial action. And if this action is not forthcoming, then supervisors can reflect this in their overall supervisory assessment of a bank, with possible consequences for the amount of capital that the bank has to hold against its risks or for the imposition of restrictions on business expansion. In some countries, the supervisors may go further into enforcement territory, imposing fines on banks with inadequate systems and taking actions against specific individuals performing senior management functions in the bank.

MORE INFORMATION
Giles Williams
Partner, Financial Services
Regulatory Center of Excellence
EMA region
KPMG in the UK
T: +44 20 7311 5354
E: giles.williams@kpmg.co.uk

Pam Martin
Managing Director, Financial Services
Regulatory Center of Excellence
Americas Region
KPMG in the US
T: +1 202 533 3070
E: pamelamartin@kpmg.com

Simon Topping
Partner, Financial Services
Regulatory Center of Excellence
Asia Pacific (ASPAC) Region
KPMG China
T: +852 2826 7283
E: simon.topping@kpmg.com

Governance strategies for managing the data lifecycle: Knowing when to fold versus hold and protect

Atul Subbiah, KPMG in the US
Sandeep Kurne, KPMG in the US

Regulatory risk management is an increasingly critical challenge for financial services firms. While credit and market risk have always featured on senior management's agenda, external regulatory developments are placing greater emphasis on effective risk management frameworks and also increasing the focus on data retention required for compliance. As a consequence, much greater attention now needs to be given to the fundamental data underlying these records and the risk associated with their retention. Experience shows that the quality and integrity of data can by no means be taken for granted. Getting it wrong could become very costly.

Focus on data governance

Financial services firms are under mounting pressure to manage regulatory compliance and associated risk more effectively. With the advent of the new Basel III regime, as well as restrictions laid down by national regulators like the Financial Industry Regulatory Authority (FINRA) and the *Dodd-Frank Wall Street Reform and Consumer Protection Act* in the US, the process of correctly identifying as well as utilizing the 'right data' for controlling risk has become a critical one.

To comply with regulatory requirements, firms will need to increase their governance in ways which conform to the new compliance requirements, improve the quality of data and optimize accumulation of new risk data. Assessments of risk depend fundamentally on data: data on counterparties, markets and internal operations. Thus far, data quality issues have been low on senior management's priorities. The new emphasis on regulatory risk management means that the governance of reference data utilized for holistic risk calculations has become a critical issue.

Regulators are focusing more closely on data, management and systems. They understand that management's ability to control the business, and quantify and manage risk, depends on the quality of relevant data available – and they are, with some reason, becoming more concerned about the poor standards of data management they are encountering. So while there is a regulatory push for improvement on one side, it is because there is also major potential benefit to be secured on the other side in the form of improved business capability.

The challenge and the benefits

The challenge is ever more acute. The volume of relevant data is soaring exponentially and much of this is unstructured and unmanaged. At the same time, retention requirements associated with regulation and litigation are compounding the problem. The potential business benefit from better data governance and management is clear. Firms can achieve improved risk management and reduced data storage costs, as well as a substantial increase in regulatory compliance, with more effective data retention and quality assurance strategies.

Contacts (from left)
Atul Subbiah
Sandeep Kurne

The collection, evaluation and retention of data, in particular records, can be particularly difficult. However, it can be optimized through strategic and effective data lifecycle governance: demonstration of authoritative sources; rational and defensible disposal of redundant and out-of-date data; and improved data quality standards. A successful data lifecycle governance program can help organizations contain costs, retain the right data and address regulatory compliance requirements. Equally important, it can increase the business value of data by providing a sounder platform for decision-making.

When aggregated across hundreds or thousands of systems, applications and databases, individually small benefits can create significant benefits overall. The main areas of potential benefit include:

- **Eliminating redundancy:** Very commonly, multiple copies of reference data are held at different points in the organization; copies of transaction data are duplicated in different environments; unrestricted end-user rights result in both duplication and inconsistency. Rationalization of data and applications within an overall data strategy can yield substantial savings: KPMG analysis suggests typical benefits of US$500-1,000 per application server and up to US$10,000 per database. In addition, more effective data governance should yield improved process and reporting accuracy, improved data quality and improved management of support resources and tools, all with clear business benefits.
- **Minimizing over-retention:** Typically, organizations hold onto data for too long as a result of retention limits not being enforced, over protective interpretation of legal requirements and over-engineered business assurance systems. Streamlined dispositions frameworks, workflow processes and assurance strategies can cut the cost of over-retention dramatically. Analysis by KPMG suggests potential savings in the range of 30-50 percent of storage costs. Collateral business benefits include reduced expenditure in the context of legal action, document discovery and assurance.

Key requirements

In order to ensure the accuracy of information provided to internal risk and compliance managers and external regulators, an unerring focus on data quality within the framework of an overall data lifecycle management strategy is critical. The challenge is continuous: new requirements emerge with each new product launch, acquisition or new regulation. So a strategic data lifecycle governance program will help avoid the continuing risks of data corruption and quality failure.

Key elements of the necessary approach include:

- A pragmatic approach to tackling the challenges and unnecessary costs associated with over-retention, legal holding requirements and duplication. An evaluation of the current data store consumption and the business, legal and regulatory retention requirements can help define 'quick wins'; at the same time, it can help develop a strategic plan for tackling problem areas and maintaining optimal data store utilization in compliance with legal and retention requirements.
- Examining the existing legal, regulatory and business requirements for data alongside the people, process and technology controls in place will allow the identification of gaps in the performance of different functions within the organization. When these gaps are evaluated against future goals, organizations can better define a data lifecycle governance structure and policies for record management.
- Data profiling is a collection of key analytical techniques that allow an organization to evaluate how effectively their core data sources contribute to a sound understanding of the underlying metrics and characteristics of the business. By analyzing the structure and content of separate data collections and comparing their outcomes, profiling can point out anomalies, deviations and variations which might suggest underlying data quality problems.

Data quality assurance

Implementing an effective data governance strategy is not a matter of mounting a one-off initiative. Sustainability of data quality assurance requires a collaborative governance program between business and technology with a joint functional concentration on data quality. Sustainability is a key component of the regulatory evaluations of an institution's reference data management framework.

A data quality assurance system underpins and reinforces the continuing value of a data governance strategy. An appropriate high-level design outline will recognize the following objectives:

- obtaining clarity and consistency on data definitions and data quality
- identifying data ownership (both content owners and distributors)
- highlighting explicit do's and don'ts about the data to be used, its authoritative source and timing
- expressing, resolving, escalating and enforcing priorities based on agreed metrics
- identifying data tools and processes to record and manage issues, action items, decisions and dependencies
- establishing clear communication channels and decision making processes for early resolution of data quality issues.

An effective approach involves defining the business rules, attributes, standards and data flows and working in partnership with cross functional stakeholders including technology, risk, finance, legal and compliance.

Conclusion

Regulatory risk management depends critically on the value of the data underlying produced records, its analysis and evaluation. Where data quality is inadequate, risk and compliance management lacks a strong foundation. Regulators are increasingly probing the adequacy of companies' systems for data retention, aggregation and analysis. Responsible oversight by senior management and boards requires that these issues are given appropriate priority.

Figure 1: Savings and benefits of proper data governance*

Cost driver	Characteristics	Common siloed responses	Savings opportunity	Benefits
Redundancy	• copies of reference data across disparate environments	• application rationalization	• approximately US$500-1,000 per app server	• improved process and reporting accuracy • improved data quality • centralization of support resources • rationalization of tools • simplified data ecosystem
	• copies of transactional data	• data rationalization	• approximately US$5,000-10,000 per database	
	• data mart sprawl	• data strategy		
	• unrestricted end-user entitlements	• enterprise maintained access methods		
Over-retention	• unenforced retention limits	• disposition framework, contract and process	• 30-50 percent of storage costs	• reduced e-discovery fees • reduced external legal expenses • reduced legal exposure • reduced BAR costs
	• slow or non-existent release of legal holds	• legal hold workflow process		
	• over-engineered backup, archive and recovery (BAR) keeping full copies of data for all production systems	• BAR Strategy		
Performance	• high-performance service-level agreements (SLAs) on historical data that keep all data 'hot'	• SLA review • 'cheap and deep' storage tier • archieve aware query management		• reduced application storage costs

*Source: KPMG analysis, 2014

Illustrative successes
In data governance engagements with clients, KPMG member firms have:

Defined a sustainable engagement model between technology, legal, business risk and compliance functions.

Developed a predictive financial model to project potential multi-year cost savings for firm's 3,000 plus systems.

Identified over 450 terabytes of duplicate and over-retained data eligible for defensible disposition.

Successfully remediated reference data quality issues related to Foreign Account Tax Compliance Act, account versus party site address and legal entity.

Achieved an annual run-rate cost reduction of US$2 million and additional storage cost avoidance opportunity of US$20 million.

Provided a holistic view of quality by issue as well as a focused indicator of quality by data element.

Addressed regulatory requirements for operational risk through successfully demonstrating an understanding of data flows and adherence to firm's record-keeping obligations for approximately 35 core systems.

Executed data quality rules in the Informatica Data Quality (IDQ)tool, enabling reuse of queries and rules for periodic measurement and monitoring of quality by rule.

MORE INFORMATION
Atul Subbiah
Principal
KPMG in the US
T: +1 212 954 3136
E: asubbiah@kpmg.com

Sandeep Kurne
Director
KPMG in the US
T: +1 212 872 2197
E: skurne@kpmg.com

Rebuilding and reinforcing risk data infrastructure

Sascha Chandler, KPMG in Australia
Marco Lenhardt, KPMG in Germany
André Lattemann, KPMG in Germany
Brian Hart, KPMG in the US

Contacts (from left)
Sascha Chandler
Marco Lenhardt
André Lattemann
Brian Hart

One of the main features of the financial crisis was that it revealed the inadequacy of banks' risk data systems and processes. This had serious impacts both on managements' ability to understand and manage risk and on regulators' attempts to maintain liquidity and limit contagion. Regulators are now seeking to instill more responsible and effective practice. Banks need to review and improve their risk infrastructure. But there are benefits to be obtained which should outweigh the costs.

Over the years, management systems in banks – and other financial services companies – have had to cope with increasing regulatory requirements, new corporate structures, new products and operating models. As with other infrastructure, systems for the collection, aggregation and analysis of risk data have typically developed in an incremental fashion, with different modules, incompatible data and a range of ad hoc processes. In many cases, these systems have become so unwieldy and unstable that they are failing in their core purpose. Relevant data is missing or inadequately analyzed, often resulting in the formation of 'reconciliation industries' within the organization as data is passed between a multitude of systems across inconsistent integration mechanisms. The extent to which these reconciliation industries have evolved within organizations is often underestimated and rarely quantified in terms of productivity loss. Risk data is being provided too late to influence the trading and operations which should depend on it. Responsible management and supervision are both compromised while operating costs are inflated unnecessarily.

> "Major market participants could not extract the necessary information quickly enough to understand the location and extent of risks and exposures.

Increasing regulatory attention

Regulators have become increasingly concerned about the implications of these inadequate or misleading risk data systems. Their shortcomings were exposed at the height of the financial crisis when regulators asked for up-to-date assessments of risk and exposures. Many institutions were unable to provide the data required or found themselves coordinating a massive manual and ad hoc intervention to assemble the data demanded of their management teams and regulators. Major market participants could not extract the necessary information quickly enough to understand the location and extent of risks and exposures. This was one major cause of the catastrophic collapse of confidence in the global financial system.

As a result, regulators are now focusing not only on the results and outcomes of risk figures but also on the machinery and processes behind them. In 2009, the Basel Committee on Banking Supervision (BCBS) issued supplemental Pillar 2 (supervisory review process) guidance designed to enhance banks' ability to identify and manage bank-wide risks;[1] and in 2013, the committee published a set of principles to strengthen risk data aggregation capabilities and internal risk reporting practices, along with guidance on their implementation.[2]

The principles, which provide qualitative and quantitative measures, cover four key areas:

- The importance of boards and senior management exercising strong governance over a bank's risk data aggregation capabilities, risk reporting practices and IT capabilities.
- The accuracy, integrity, completeness, timeliness and adaptability of aggregated risk data.
- The accuracy, comprehensiveness, clarity, usefulness, frequency and distribution of risk management reports, including to the board and senior management.
- The need for supervisors to review and evaluate a bank's compliance with the first three sets of principles listed above, to take remedial action as necessary and to cooperate across home and host supervisors.

1 Basel Committee on Banking Supervision (BCBS), *Revisions to the Basel II market risk framework*, July 2009, BCBS158, www.bis.org/publ/bcbs158.pdf.
2 Basel Committee on Banking Supervision, *Principles for effective risk data aggregation and risk reporting*, BCBS239, www.bis.org/publ/bcbs239.pdf, January 2013

Key issues

Where banks have undertaken systematic analysis and testing of their current processes, the results have often been illuminating. In certain cases, it has revealed that compiling a comprehensive group-wide set of risk figures has been taking up to 60 days. The larger and more complex a bank, the more likely it is that risk data is incomplete, inadequate or out-of-date, particularly on an aggregated and global level. Banks may have all of the information, but it's often inefficiently stored, inconsistently formatted, poorly integrated and difficult to interrogate. Senior management should be aware of the risk of 'flying blind', especially in extreme events, and of taking and implementing decisions in the absence of reliable risk metrics. It is critical, therefore, that financial services firms review the strength and effectiveness of their risk data architecture and systems.

There are four key issues which need to be addressed:

- **Efficiency:** very often, data resides in different silos, owned by different functions (markets, risk control, finance, back-office), all with different attitudes and approaches to data management. With multiple systems and incompatible data, risk professionals spend too much time and effort on data aggregation, reconciliation and analysis and too little time on applying the results to risk management and decision-making.
- **Flexibility:** It is important to be able to react quickly to market events in terms of preparing scenario analysis and reports which are not in the standard setup. Similarly, the flexibility to react rapidly to regulators' requests for reports and data without a huge amount of manual work is also important.
- **Quality:** With multiple, discrete systems, the quality of data is degraded by incompatible definitions, inconsistency, incompleteness and duplication. Very often, efforts in data cleansing are only partially successful. With poor quality data, the effectiveness of risk management can be seriously compromised.
- **Ownership:** Too often, ownership of risk data is shuffled uneasily between the control function and the IT function, with senior management taking little direct responsibility. Without a clear structure of governance and ownership there is no accountability and no prime commitment to quality.

Four issues banks need to consider when reviewing their risk data architecture and systems:

Improvements and benefits

This review of common problems naturally also suggests the scope for improvement and the value that can be obtained from effective risk data aggregation, storage and analysis. The ability to consolidate and synchronize all relevant risk data can lay the foundation for a more overarching and consistent analysis, enabling better business management, better risk management and optimized operating models. Leading banks appreciate the potential benefits and are working to strengthen the contribution of effective risk management to business judgment and corporate strategy.

High-quality and quality-assured risk data should lead to improved decision-making, greater confidence and more stable strategy. With greater confidence in data validity, risk IT architecture can be streamlined, leading to efficiencies in both routine operations and in maintenance and development. In turn, these benefits offer improved ability to respond quickly and effectively to changes in corporate strategy, operating environment or, indeed, regulatory demands. If regulators have greater confidence in a bank's risk data and the aggregation machinery underlying it, the whole regulatory compliance system can become simpler and less challenging.

Improved data aggregation can bring direct economic benefits and reduced capital requirements. Currently, for example, a significant proportion of a bank's collateral contracts are ineffectively captured and so cannot contribute to risk-weighted capital calculations. More comprehensive and accurate data aggregation methodology can bring this into the equation.

Systems for transmitting and reporting risk data need to be built into any improved data aggregation framework since its value is dependent on the ease and timeliness with which senior management can take the results into account. The same argument applies to communication with regulators, who will value rapid and accurate regular reporting as well as a speedy response to ad hoc requirements.

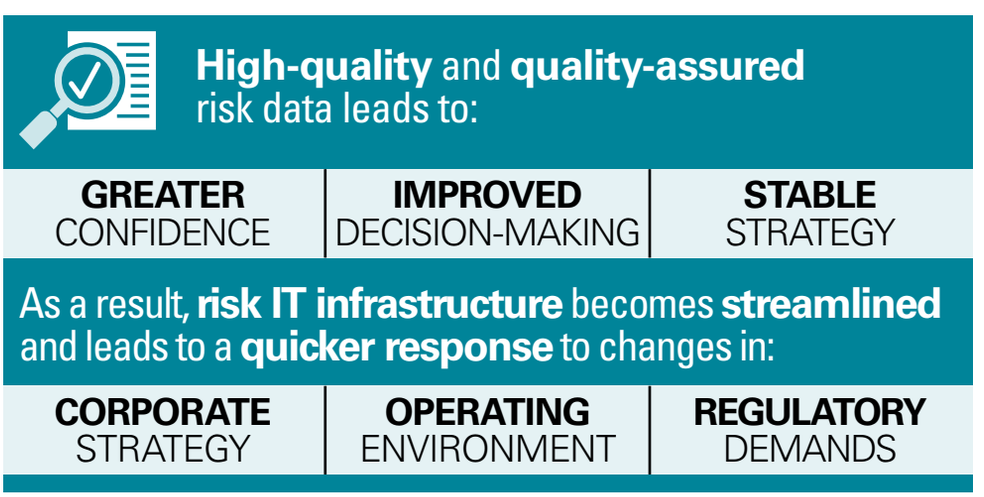
Achieving the benefits requires moves towards greater standardization, common data models, integrated systems and, in some circumstances, consolidated data warehouses. These initiatives need to be defined and implemented in ways which balance costs and potential benefits. But since the results should include increased confidence, reduced potential for loss, efficiency gains and increased profits, significant effort and expenditure can often be worthwhile.

Conclusion

Risk data aggregation and reporting are too important to be left to the risk function or – more seriously – IT professionals. Regulators are demanding better performance, but equally, senior executives and boards will derive significant benefits from improving their risk infrastructure and processes. However, this is not a simple or straightforward challenge. Success requires fundamental changes in the way core functions operate, with significant potential consequences for organization and processes. Inevitably, this can be expensive. However, effective renovation of the risk IT infrastructure is a strategic investment which not only satisfies regulatory demands, but also leads to competitive advantage.

Responsible governance, therefore, requires that these issues are given appropriate strategic attention at the highest levels.

“Risk data aggregation and reporting are too important to be left to the risk function or – more seriously – IT professionals. Regulators are demanding better performance, but equally, senior executives and boards will derive significant benefits from improving their risk infrastructure and processes.



MORE INFORMATION
Sascha Chandler
Director Financial Risk Management
KPMG in Australia
T: +61 2 9455 9596
E: schandler@kpmg.com.au

Marco Lenhardt
Partner
KPMG in Germany
T: +49 69 9587-3403
E: mlenhardt@kpmg.com

André Lattemann
Senior Manager
KPMG in Germany
T: +49 69 9587 3988
E: alattemann@kpmg.com

Brian J. Hart
Principal
KPMG in the US
T: +1 212 954 3093
E: bhart@kpmg.com

Seeing is believing: Visual Analytics and making sense of data

Dai Duong, KPMG in the UK
Spencer Marley, KPMG in the UK

Financial organizations face ever-increasing demands on performance against a background of constant change. Effective responses depend more and more on the capacity for deep and rapid understanding of business operations and performance. Traditional information systems can sometimes suffer under the strain of a rapidly changing environment. However, new technologies can now deliver radically improved results.

Everyone involved in the financial services industry is aware of the rapid and increasing pace of change affecting all aspects of the business environment. Of course, there are major regulatory changes which have just been implemented. But there are also significant and continuous changes – both strategic and operational – following industry restructuring, new business models and the attempt to recover stability in a post-crisis world.

Understanding the needs

All of these changes place a premium on agility: the ability to respond rapidly and effectively to an unpredictable environment. Businesses can only act by having a more responsive and detailed understanding of the business. Information on costs and margins is needed at a much more granular level. The need to manage risk better in an environment where change happens rapidly also calls for more accurate and timely data. Current management information systems often fail to measure up to the challenge. They do not aggregate the right data at the right level quickly enough. Furthermore, they are ineffective at gathering and reconciling data from multiple sources. As finance, operations and risk functions all have separate data systems, forming a coherent overview between systems is often impossible.

Rapid and accurate data collection is only part of the challenge, however. Ensuring its accessibility in real time to the relevant decision-makers is also critical. Many senior users of management information spend substantial periods of time away from their desks, either traveling or in meetings. Global companies operate across many different time zones. Solutions that offer constant mobile access to crucial data are essential.

To meet the challenge, companies need robust, flexible solutions that can be rapidly deployed in a matter of weeks or months, not years. An agile solution needs an agile approach to understand the underlying business issues. This requires locating relevant data and creating a data model, preparing analytics and dashboards and facilitating sharing and collaboration across the organization.

Understanding the technology

While there are many existing technologies that seem to deliver business insights, few are agile in nature. The problem is threefold. First, data is not usually accurate, timely or relevant

Contacts (from left)
Dai Duong
Spencer Marley

enough. Traditionally, finance, operations and risk functions have all had separate data systems, which make having a coherent overview of the business difficult to achieve. Senior executives need to have available reliable information on what happened yesterday and not that from 2 months ago. Second, even if real-time data is available, users are not able to view the data in a form and at a level of detail that they require. Financial institutions typically collect key operating data in massive bespoke management information systems that generate static reports based on a fixed schedule. This means businesses need to spend more time conducting further analyses, which slows down their response. Consequently, they may not receive the insight they need to respond effectively. Finally, even if such technology is available, it usually takes too long to implement. Before going live, the technology may already be irrelevant. Given the rate and magnitude of changes in the financial services industry, companies need agile data, technology and implementation.

In recent years, however, major advances in computing power and software development have made a number of helpful products commercially available. These products simplify and streamline the task of extracting management data and build on this data to create insightful and timely information and reports. Products such as QlikView[1], Tableau[2] a Microsoft business intelligence stack[3] and TIBCO Spotfire[4] are revolutionizing how companies can aggregate, analyze and report their financial and operating data.

So how do these products work? They work by adding an analytical and visual overlay on top of existing systems. With these products, agile data is now available, as many disparate data sources can be linked across the firm to present a single version of the truth. Agile technology is now available as large volumes of information can be stored into local memory so that users can conduct rapid analysis on a preloaded set of data. Doing so using an intuitive visual front-end means anyone in the business can ask any question they have whenever they want and get relevant answers. Agile implementation is now available since dashboards created by these products builds on, rather than replaces, current systems. Implementation can happen in weeks and months rather than the years it would take to develop a completely new management information infrastructure. These solutions are also scalable and can be implemented in shorter time phases if necessary. These tools can be used as an end-to-end solution for businesses that are willing to invest in such technology or as a prototype for others that would like to try these products out.

The potential benefits

Not only are these kinds of solutions cost-effective to implement, but they save money on a continuing basis. They can dramatically decrease the time and effort spent on aggregating, reconciling and cleaning data from disparate sources. With a single real-time view of the truth, there is no need for debate about which numbers are valid. Management can then focus on genuinely valuable analysis instead. In delivering insightful analysis rapidly to key decision-makers, wherever they are, these tools help improve business performance.

At KPMG member firms, we have leveraged such technology and applied visual analytics both in our own internal operations and in delivering effective solutions to client requirements.

Visual Analytics

Visual Analytics put visual information into the hands of key users, bringing together various data sources intuitively to create reports and dashboards. A single graphic can tell a story that may otherwise be embedded in a complex spreadsheet.

In effect, rapid development can be achieved with pre-built modules that can be deployed with limited customization; many tools can be largely re-used as-is as building blocks for bespoke solutions; modular development supports remixing and reassembly to meet changing needs over time.

Characteristic Visual Analytics applications have included:

- An **investment management dashboard**, which allow users to view overall assets under management and readily 'slice and dice' by asset class, region, fund type and currency; at a click analysis can drill down to fund level, client portfolio or fund manager performance.
- A **banking workforce analytics dashboard**, which looks holistically across all workforce data (cost, capability, compliance, talent and engagement) as part of a program to improve financial performance, customer experience, risk and employee engagement. Now banks can manage their workforce to enhance employee engagement and customer experience while maximizing the financial performance of the business.
- A **management information tool**, which allows users to view the performance of a business at various levels by teams, functions and across organization; this is linked directly to multiple data sources and is accessible by thousands of users for better decision making. Now, management can easily ask and answer their own questions using iPads in board meetings, without delays or reliance upon a finance team to produce reams of static portable document format (PDF) reports.

These new business discovery tools allow senior executives faster access to the important data underlying business performance presented in a genuinely insightful manner. The ability to recast information instantly from different perspectives can reveal surprising and original insights, allowing the organization not only to respond to rapidly changing demands but also to identify opportunities for step-change improvements in performance. With insight and industry experience, these tools can deliver dramatic impact for the business relative to both effort and cost.

MORE INFORMATION
Dai Duong
Director
KPMG in the UK
T: +44 20 7311 6332
E: dai.duong@kpmg.co.uk

Spencer Marley
Senior Manager
KPMG in the UK
T: +44 20 7311 5862
E: spencer.marley@kpmg.co.uk

1 ®Qliktech International AB http://www.qlik.com/
2 ®Tableau Software Inc http://www.tableausoftware.com/
3 ®Microsoft Corporation http://www.microsoft.com/en-us/default.aspx
4 ®TIBCO Software Inc http://www.tibco.com/

Technology and payments:

Beyond the hype?

Georges Pigeon, KPMG in Canada
Tim Johnson, KPMG in the US
Jeremy Welch, KPMG in the UK

There is tremendous activity at the moment in the payments sector driven by advances in communications and associated technology. Financial services companies, payments companies and new entrants alike are making major investments, launching innovative new initiatives and jostling for leadership in what is a rapidly changing market. However, it is far from clear that anyone has identified a winning proposition that will be able to dominate the market. Providing real benefit to the consumer will be key to widespread adoption of new platforms.

Contacts (from left)
Georges Pigeon
Tim Johnson
Jeremy Welch



Payment services have historically been a relatively stable sector of the financial services industry; at best, they are an after thought. Significant developments and progressive changes in the background and in back-office systems have been implemented in recent years; yet, there have been few really great leaps forward with a major impact on the consumer experience since payment cards (charge cards, credit cards, payment cards) began to supplant checks and become an alternative to cash 50 years ago. However, all that looks set to change.

The last 2 years have seen a growing number of initiatives in the payments sector, especially in mobile payments technology. The range and variety of current developments is extensive and potentially quite confusing. What is less certain is which, if any, of this multitude of initiatives will have the potential to penetrate mass markets and truly transform consumer behavior.

Drivers of change
There are drivers of change from many directions:

- Consumers have been progressively moving away from the use of cash for decades. In advanced consumer societies in North America, Western Europe/Scandinavia and Asia, the use of checks has dwindled in favor of payment cards of various types. Payment by cash is now largely restricted to small value retail purchases. Even here, the indications are that consumers would embrace simple-to-use, reliable, cash-free payments methods with alacrity.
- Merchants who use point-of-sale card terminals typically pay fees of 2-5 percent of gross sales value to credit card companies and acquirers for credit card use and a lower rate for debit card acceptance. Their judgment is that this is, at present, a necessary cost to bear in order to allow customers to pay them without incurring the additional inconvenience of cash. From the merchant's point of view, card acceptance has some advantages in reducing cash needs and the risks of crime, but 2-5 percent is a high cost to bear. The pressure exerted by Congress via the Dodd-Frank Act and the remit of the Commodity Futures Trading Commission to oversee a reduction in interchange and the cost of 'loyalty cards' has triggered a shift in this market. There is no doubt that cheaper payment alternatives would find a widespread market.
- Small traders and craftsmen, for example in the building trades, domestic services and those operating without a fixed home base, have historically had few options for efficiently and cost effectively receiving payment beyond cash or checks, each of which has significant drawbacks. There is massive pent-up demand here for more efficient, streamlined and low-cost systems that provide reconciliation data that can be integrated into their accounting software back to small businesses around the collection of funds. Tax authorities would also probably favor more traceable payment mechanisms from the perspective of reducing tax evasion.
- Recognizing these pull factors and faced with the threat of disintermediation by new technology-based start-ups that ignore the wider banking relationship, banks and other financial services companies see both major opportunity in introducing innovative payment systems to satisfy the latent demand and a clear threat if they don't innovate to serve a sizeable and lucrative small and medium enterprises market.
- Card companies, perhaps the market participants most threatened by transformational payments technologies, have stronger interests than many in controlling the direction of innovation. Payment networks, card-issuing companies payment processing companies and banks all face differing challenges and some may be more exposed than others.
- Given the potential for substantial market disruption, there are obvious attractions to many classes of new entrants who might be able to develop a winning proposition.

One of the major enablers is technology. Two areas have proved especially significant. The first is near field communication (NFC). Earlier radio frequency identification (RFID) allowed enabled devices to operate as contactless payment methods. Contactless smart cards have been in use in many parts of the world for over a decade. However, in some markets, adoption was initially limited by unreliability and by the need for significant capital investment by retailers. NFC extends the technology by allowing higher capacity two-way communication between devices. These can function as contactless payment systems as before, but can also form the basis for more advanced and reliable systems.

The second key enabler is the platform of advanced technologies now available in smartphones, tablets, other portable devices and mobile communications. Apart from enabling remote communication with banks, card companies, supplier bases, etc. global positioning (GPS) technologies can locate consumers accurately and push much more relevant data and information to them. Together, NFC and mobile technologies provide the foundation for significant further advances in payments systems, which are attracting attention and investment from many directions. Hardly a month passes without a new product or platform announcement, a new industry partnership or a new entrant promising a radically new approach.

Recent developments
Some key recent developments include.

- **Barclays Pingit** allows holders of any current account in the UK to transfer and receive money using any Android or iOS device. Small business operators and traders can use Pingit to get paid instantly by customers. Consumers can transfer cash between friends and family members, split bills in restaurants and so on. Pingit uses the UK's Faster Payments Service, introduced to radically reduce transfer and clearing delays, so payments are effectively instantaneous as well as free. Barclays also hopes to attract new customers for its wider banking services.
- **New entrants** such as Moven (from Movencorp Inc. in the US) and Ontrees are also competing directly with the banks by offering a combination of mobile banking and payments services via smartphone. Ontrees integrates data from customer bank accounts and purchase transactions,

allowing a variety of analyses, services and presentations of financial information. Moven offers comparable benefits, combined with a payment infrastructure based on both debit card and RFID.

- **Point-of-sale** is traditionally the world of credit and debit card companies and acquirers. A number of retailers are introducing or have introduced new payment options based on mobile phone apps and NFC, including Starbucks in the US and Canada. In the UK, MasterCard recently announced a partnership with Weve (owned by Vodafone, Everything Everywhere (EE) and Telefónica UK (O2)) to develop a comprehensive contactless mobile payments system. However, the introduction of contactless NFC terminals has not been problem-free and there have been complaints over reliability and security.
- **Zapp:** Also in the UK, VocaLink, which already operates Link, one of the largest ATM networks and provides the infrastructure for clearing services for credit transfers and Direct Debit is launching Zapp, which will allow retail customers to pay for purchases via a mobile application loaded on their smartphones.
- **Systems targeted at small businesses and sole entrepreneurs** include Square Register from Square, Inc[1] in North America and iZettle, a Swedish company currently operating in a number of European and Latin American territories. Both solutions involve extending the range of existing payment card technology with the use of a card reader; this plugs into the audio jack of a smartphone and allows it to read either the magnetic stripe or the chip on the payment card and communicate with a payment provider. In 2013, iZettle formed a partnership with Santander. Intuit, who market the QuickBooks accounts software for small businesses in the UK and PayPal, eBay's global payments services provider, have both introduced similar services.
- **eBay acquisition of Braintree:** In September 2013, eBay acquired the payments provider Braintree, whose Venmo app supports payments by tablet and smartphone for US$800 million. Braintree will operate within eBay's PayPal business, strengthening its capability in mobile systems. At the same time, the acquisition eliminates a rapidly growing competitor. As PayPal continues to explore NFC, the company is developing a virtual wallet and the ability to support peer-to-peer transactions.
- **Klarna acquisition of SOFORT:** Also in 2013, the Swedish online payment services company Klarna acquired a German rival, SOFORT, for more than EUR150 million.

However, the very range of current developments testifies to an immature and uncertain market. It is clear that only a very small number of these innovations will prove to have the winning combination of customer benefits, ease of use and economic advantages to survive. Markets simply cannot support a large number of inconsistent and conflicting payments systems. Regulators, too, should increasingly drive consistency and standards to protect consumers, such as under the Payments Services Directive in the European Union.

Extracting value

Advanced payments systems are having to break into a market which is inherently low margin. The transaction fees which can be earned directly from providing payment services are, however, not the primary attraction. The potential value lies in control of the consumer interface and the access it provides: to customer and market data and the ability to target added value services, advertising and promotions directly to the customer at the right time in the right place. In effect, payment data is more valuable than payment fees: payment transaction data can generate value for all of the participants in the payments value chain.

This potential is why the payments battlefield is particularly fiercely contested at the moment. As we have seen, banks, card companies, new entrants, mobile telecommunications companies, hardware suppliers are all in effect fighting to take control of consumers' day-to-day spending and payment operations and exploit that control as the basis of higher value, higher profitability services. Technology and applications that can exploit payments data, for example, in delivering assessments of payment

1 Square Inc also powers one of the mobile phone payment systems operating in Starbucks

information quality or customer and marketing analytics, can help develop marketing strategies and inform audience segmentation.

Many of the competing technologies have different, very powerful backers, that are all jockeying for position. But they will not necessarily be able to impose a solution on the public. It may be that telecom carriers, hardware providers or card networks will determine the future of payments technology rather than banks themselves. However, for new payment technologies to be seen as more than a gimmick and for consumers willingly to adopt them, more needs to be done to identify systems that will add value for the user as well as for the provider.

To attract consumer take-up, alternative systems will have to compete effectively with the simple or virtually costless alternatives of using plastic or carrying cash. While each of these carries some theoretical risk (loss, robbery, fraud), in practice the risk is small. And, by definition, the acceptable economic cost of a payments system is limited to a small proportion of the value of the underlying transaction. Will consumers switch in droves to new technologies? Despite the hype and the major investments now being made, new systems may face an uphill challenge.

> Markets simply cannot support a large number of inconsistent and conflicting payments systems.

MORE INFORMATION

Tim Johnson
Partner
KPMG in the US
T: +1 312 665 1048
E: tejohnson@kpmg.com

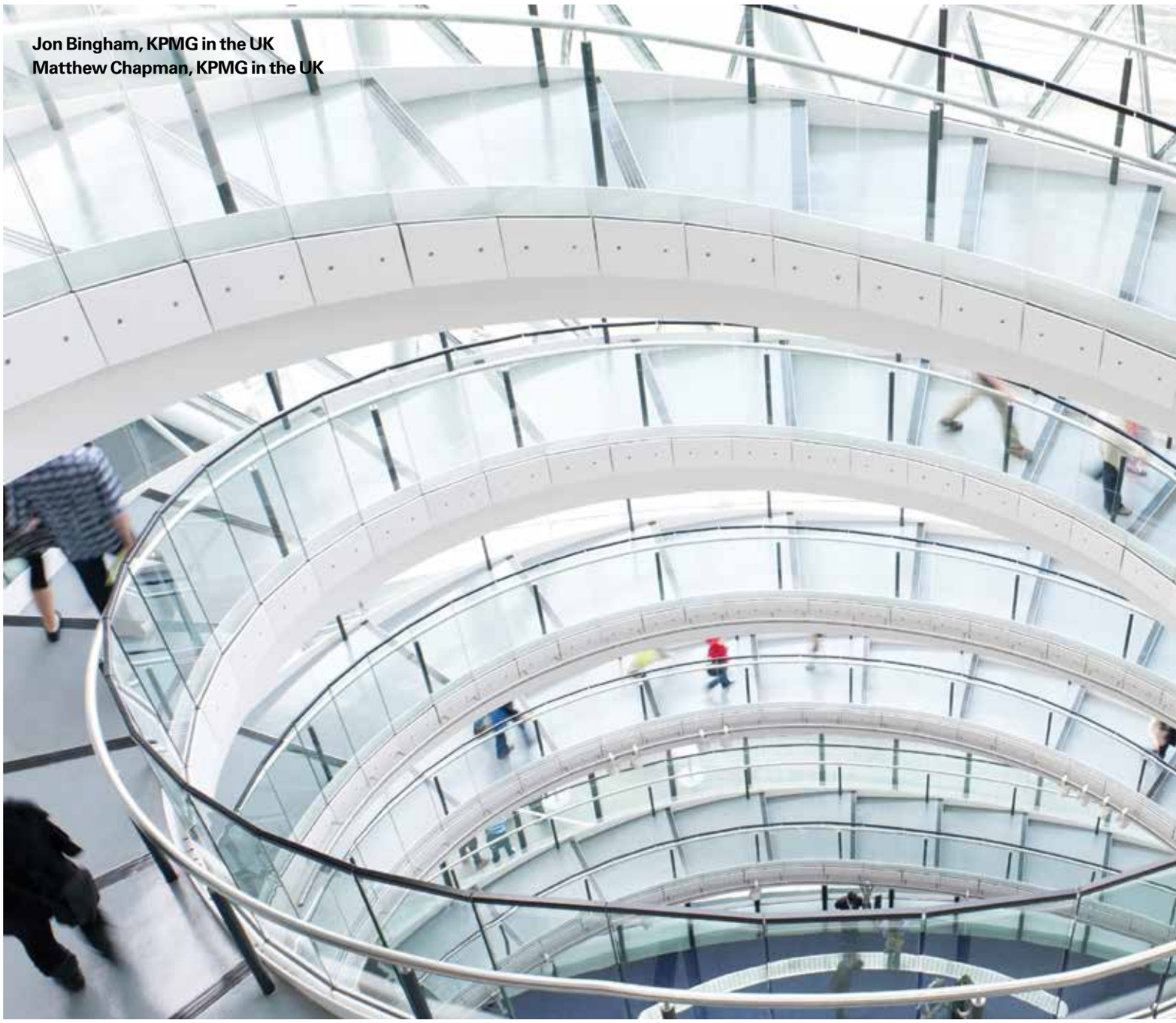
Georges Pigeon
Partner
KPMG in Canada
T: +1 514 840 2178
E: georgespigeon@kpmg.ca

Jeremy Welch
Director
KPMG in the UK
T: +44 20 7311 2527
E: jeremy.welch@kpmg.co.uk

Better bank reporting:

Aligning reports with shareholder value

Jon Bingham, KPMG in the UK
Matthew Chapman, KPMG in the UK



Contacts (from left)
Jon Bingham
Matthew Chapman

> More attention now needs to be given to rationalizing overlapping disclosures and building on the recent (largely positive) disclosure enhancements more explicitly.

Banks' annual reports are groaning under the weight of new disclosure requirements. While their financial statements have become significantly more transparent and consistent, it is becoming more difficult to discern the overall message. Investors are presented with an abundance of financial data, but struggle to identify relevant information. It is now time to take a step back to consider how annual reports could do more to help banks communicate their business story to investors; and to re-examine the most effective boundary between the contents of annual reports and other information provided to stakeholders (Pillar 3, analyst presentations, website disclosures etc.). Aligning reporting with shareholder value is a challenge in every sector, but the volume and technical nature of bank reporting makes it especially difficult.

The challenge is particularly timely when many in the sector are in the process of refocusing their business models to restore public and shareholder trust. In the main, this has reduced complexity in banking businesses, but the complexity of the message to investors has increased – partly in response to uncertainty over the regulatory agenda. Better business reporting is necessary to demonstrate how the changes banks are making to their business models are helping to protect and develop shareholder value and ultimately to enable financial capital to find those businesses that are most able to create value.

Bringing focus to reports

Annual reports are being asked to be more consistent across the sector while also becoming more tailored to the individual bank's circumstances. In this situation, the value of simply adding more and more detailed financial analysis is increasingly limited. More attention now needs to be given to rationalizing overlapping disclosures and building on the recent (largely positive) disclosure enhancements more explicitly. The decluttering actions being taken by many banks can help here by drawing out the most relevant financial information. Conversely, if the banking sector is able, over time, to restore trust in the relevance of the information it reports, there may be an opportunity to break out of the circle of tightening disclosure obligations.

The focus of reporting development is now starting to shift beyond just the financials. In the UK, for example, impetus is likely to come from the Financial Reporting Council's (FRC) guidance on preparing a strategic report and from going concern recommendations. Initiatives like this may be seen in isolation as a fresh set of disclosure obligations or they can be viewed as the start of a wider evolution in the relevance of business reporting, based on a re-examination of reporting culture.

Reporting evolution in the banking sector

Source: KPMG International, 2014

This offers the opportunity for a different perspective in the report more closely aligned with a bank's own business model and more relevant to an understanding of how its prospects have been developed and protected over the short-medium and long-term. Below are three ideas for evolving banks' reports from data tables to documents that better support an analysis of shareholder value. These ideas build on recent reporting developments in the sector and the emerging area of integrated reporting. They also draw on the wider reporting experience of other sectors.

The link between earnings and the financial risk decisions taken needs to be made more clear

More than any other industry, the risk decisions taken by a bank have an immediate impact on financial performance. They are essential context for an understanding of current earnings. Recent reporting initiatives by financial services regulators, securities regulators and industry working parties (e.g. the Enhanced Disclosure Task Force) have significantly improved the information reported on the risks being taken by banks. However, investors still need help to connect this information with its implications for current and medium-term business performance.

A significant step would be to bring an earnings focus to the extensive balance sheet risk information now being provided. Linking risk reporting with earnings performance could help investors compare underlying profitability across banks following different risk strategies.

Focus on operational performance to explain business prospects

Analysis of earnings and balance sheet risk provides part of the story of how enterprise value has been developed and protected, but a broader perspective should address the key assets on which business prospects depend. For a retail bank, development of the customer base and the operating platform will be central to business prospects. For an investment bank, a key part of value may lie in its market position, staff base and product range. The back-to-basics approach of many banks' strategies has recognized these operational assets as key drivers of value.

Bank reporting needs to catch up with these developments. Showing how key business assets, such as the customer base, have been developed and protected could support a more complete assessment of business prospects. This is an area that is beginning to evolve both in internal and external reporting. As it does so, banks need to look to the most relevant measures of performance, whether they be indicators of operational risk (such as key staff retention), indicators of progress in managing risks and opportunities (such as the status of retail branch refresh programs), or operational outcomes (such as customer churn rates). In some cases, the value of this information may lie in its comparability across the sector; in other cases, the bank's track record over time may be most relevant.

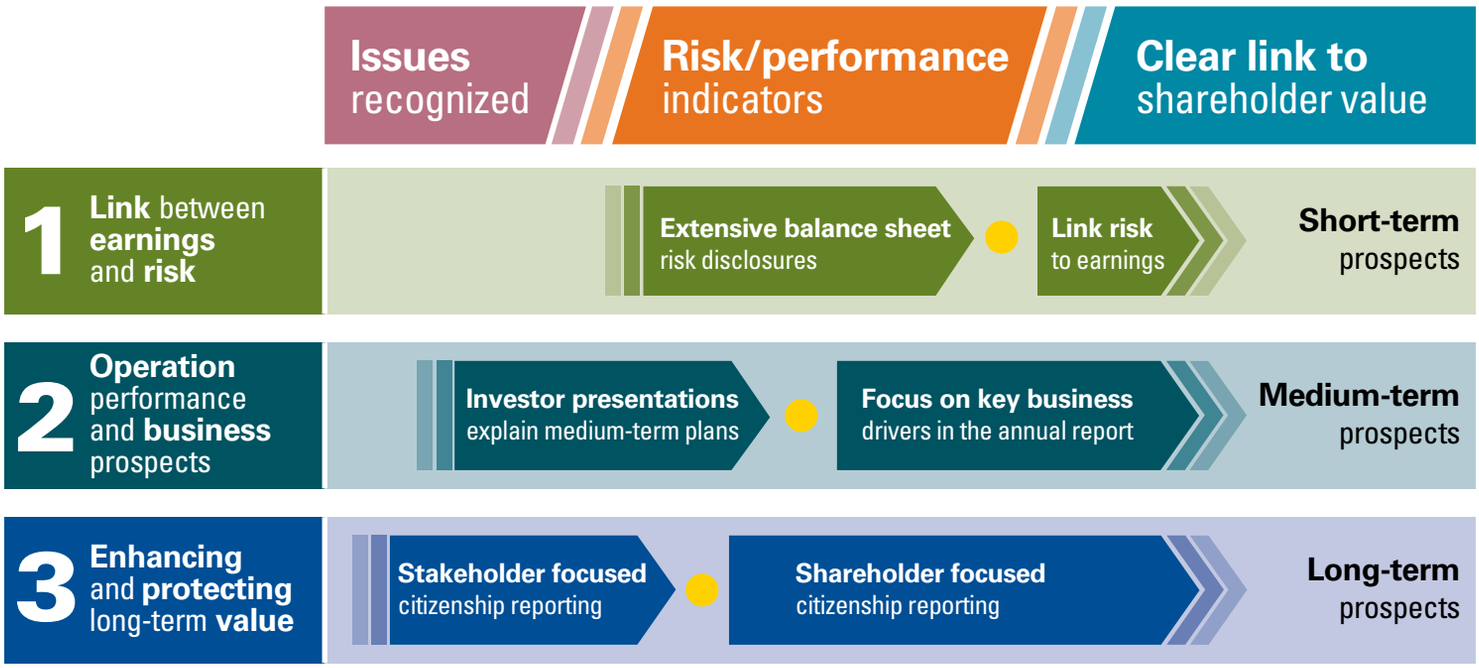
'Business as usual' cannot be taken for granted – reports should reflect this

Like any highly regulated business, banks' relationships with their customers, counter-parties, society and government should be central to their long-term future. Financial reporting requirements will continue to evolve in the wake of the financial crisis. But one of the principal concerns of investors will remain 'What are the long-term business vulnerabilities and how does the bank manage them?' Reporting needs to provide investors with credible, objective information if it is to support their assessment of the actions taken to preserve the long-term prospects of the business.

Banks are investing heavily in 'citizenship-type' reporting. However, these reports tend to focus on 'Why we are good for society?' rather than 'How we have protected shareholder value?'. The result is that they can look simply like a list of good deeds and are failing to connect with shareholder needs. Investors need objective information on banks'

> In the UK, for example, impetus is likely to come from the FRC's guidance on preparing a strategic report and from going concern recommendations. Initiatives like this may be seen in isolation as a fresh set of disclosure obligations or they can be viewed as the start of a wider evolution in the relevance of business reporting based on a re-examination of reporting culture.

Post-crisis reporting developments



Source: KPMG International, 2014

citizenship agenda to distinguish between organizations that are investing to protect and enhance long-term shareholder value and those that are prioritizing short-term financial performance. Crucial to this is understanding the fundamental implications of the regulatory uncertainties that banks are having to manage as they look to reshape their business models to meet society's changing demands on the sector. Information on banks' stress-testing can be a source of better understanding of such complex and inter-related risks.

Communicating the message

Investor presentations have developed as a means of providing the answers to some of the issues raised above. They can be more timely as they are not tied to the annual reporting cycle, but they still have a tendency to respond to short-term earnings over long-term value. Investors are looking for greater confidence that they are being provided with the complete picture. Good narrative reporting that is aligned with the organization's business model should support the reliability and completeness of the picture presented in other, more timely, communications by embedding it in the organization's formal reporting processes.

Each of these ideas is at a different stage of evolution in reporting terms. Banks need to focus on answering the specific questions raised by all three rather than looking for a single magic bullet measure of shareholder value creation based on a single financial ratio or other metric.

Developing a better business report

These ideas can form a starting point for identifying ways in which banks could improve their dialogue with investors rather than the end point. Narrative reporting should reflect the unique features of each business. For those looking to explore this further, we suggest three challenges to start the improvement journey:

- Tell your value creation story on your terms by building your reporting around your business model rather than starting from a disclosure checklist.
- Consider what constitutes a 'good year' for your business. If it is more than just meeting your earnings targets, are you giving shareholders the information to look beyond the short-term financial performance to see this?
- Ask yourself whether the information provided enables shareholders to form a view over the long-term prospects and value in the business.

MORE INFORMATION
Jon Bingham
Partner
KPMG in the UK
T: +44 20 7311 5814
E: jonathan.bingham@kpmg.co.uk

Matthew Chapman
Senior Manager
KPMG in the UK
T: +44 20 7311 3236
E: matthew.chapman@kpmg.co.uk

Publications

KPMG member firms provide a wide-ranging offering of studies, analysis and insights on the financial services industry. For more information, please go to kpmg.com/frontiersinfinance

Future of investment banking
April 2014

Investment banking has always been a cyclical business, replete with periods of prosperity and contraction. This time, however, it is different. In our view, the market has fundamentally changed. Powerful forces continue to alter the investment banking landscape in a manner and degree never before witnessed.

Evolving Insurance Regulation
March 2014

An in-depth review of the regulatory landscape with a particular focus on the growing role of new policymakers, the pressure to align insurance rules to the banking model, the rise of consumer protection laws and the latest insurance risk and accounting changes.

Global Anti-Money Laundering (AML) 2014
February 2014

How is the financial services industry rising to today's global AML challenges? This report provides an in-depth analysis of the AML landscape and a view into emerging areas of risk such as trade finance and tax evasion, as well as a look at AML trends within the insurance and asset management sectors.

Evolving Banking Regulation 2014
February 2014

An extensive review of 2013 bank regulation including the impact on bank structure, conduct and culture, data and reporting, and risk governance.

Going beyond the data
January 2014

Achieving actionable insights from data and analytics. In today's competitive marketplace, it's not about how much data you own; matters is what you do with it. This report explores the views of 140 CFOs and CIOs from major corporations around the world.

The Social Banker v2.0
January 2014

This report brings together the insights of 12 industry experts – including executives from ICICI Securities, McDonalds, RBS and NatWest – and provides new and insightful take-aways and viewpoints from KPMG's sector leaders around the world.

Towards the Final Frontier
January 2014

This report examines key business implications for insurers to consider regarding the current insurance accounting proposals.

Taxation of real estate investment trusts
December 2013

This report sets out the key regulatory, tax and legal rules for the establishment and operation of real estate investment trusts or their local equivalent in all major jurisdictions.

Cost of Compliance
October 2013

This report, which incorporates the views of 200 hedge fund manager, explores the challenges and opportunities they are facing on regulatory compliance and highlights some solutions being undertaken in the market.

The Valued Insurer: Leading the pursuit of sustainable growth
June 2013

This publication offers unique insight and opinion on emerging customer trends and channel developments in the Insurance sector. We explore the four critical attributes we believe underpin an insurers ability for success now and into the future.

KPMG Spain Contacts –
Cyber crime

Marc Martínez
Partner, Head of IT Advisory Risk Consulting
KPMG in Madrid
T: +34 91 456 59 74
E: marcmartinez@kpmg.es

José Manuel Cea
Partner, IT Advisory Management Consulting
KPMG in Spain
T: +34 91 456 60 26
E: jcea@kpmg.es

Ramón Cañete
Partner, Management Consulting
KPMG in Spain
T: +34 94 479 73 06
E: rcanete@kpmg.es

Jordi Oliver
Partner, Management and Risk Consulting
KPMG in Spain
T: +34 91 451 30 90
E: jordioliver@kpmg.es

Contacts

Francisco Uría
Partner, Head of Financial Services
KPMG in Spain
T: +34 91 451 31 45
E: furia@kpmg.es

Antonio Lechuga
Partner, Head of Insurance
KPMG in Spain
T: +34 93 253 29 47
E: alechuga@kpmg.es

Pedro González Millán
Partner, Head of Asset Management
KPMG in Spain
T: +34 91 456 35 53
E: pjgonzalez@kpmg.es

Javier Muñoz Neira
Partner, Head of Audit Financial Services
KPMG in Spain
T: +34 91 456 38 26
E: fjmunozneira@kpmg.es

Amparo Solís
Partner, Head of Transactions and Restructuring FIG and RE
KPMG in Spain
T: +34 91 451 32 25
E: asolis@kpmg.es

Víctor Mendoza
Partner, Head of Financial Services Tax
Global Head of Banking Tax
KPMG in Spain
T: +34 91 456 34 60
E: vmendoza@kpmg.es

Carlos Trevijano
Partner, Head of Financial Services Management Consulting – Strategy and Operations
KPMG in Spain
T: +34 91 456 82 42
E: ctrevijano@kpmg.es

Gonzalo Ruiz-Garma
Partner, Head of Financial Risk Management
KPMG in Spain
T: +34 91 456 60 47
E: gruiz@kpmg.es

Miguel Angel Martín Aguado
Partner, Head of Transaction Services Financial Institutions Group (FIG)
KPMG in Spain
T: +34 91 456 59 63
E: miguelmartin@kpmg.es

Francisco Gibert
Partner, Audit and Transaction Financial Services
KPMG in Spain
T: +34 93 253 29 70
E: fgibert@kpmg.es

kpmg.com/app

Available on the App Store

kpmg.com
kpmg.com/socialmedia

Produced by KPMG's Global Financial Services Practice

Designed by Evalueserve. Publication name: Frontiers in Finance – Summer 2014 – (Spain)

Publication number: 131086 (Spain). Publication date: Summer 2014. Printed on recycled material.