KPMG
cutting through complexity

Evolving Banking Regulation Part Three

Data and technology: The regulatory and business challenges

October 2015

kpmg.com

KPMG INTERNATIONAL

Contents

Evolving Banking Regulation – Parts One and Two

This publication is the third part of the *Evolving Banking Regulation* series for 2015. This report examines the data, technology and cyber security challenges facing banks.

The first part outlined the **regulatory pressures on banks**. The second part focused on bank structure, and the **search by many banks for a viable and sustainable future** in a world where regulatory and commercial pressures are driving business model change.

Future issues of *Evolving Banking Regulation* will focus on conduct, culture and governance.

Executive summary

This is the third part of this year's *Evolving Banking Regulation*. The first part covered the journey of the post-financial crisis regulatory reform agenda from development to implementation; while the second part focused on bank structure and banks' search for viable and sustainable business models.

The data and technology challenges facing banks are a natural continuation of these themes. Indeed, **high quality data and effective technology should be at the heart of a profitable and sustainable bank**.

Regulation

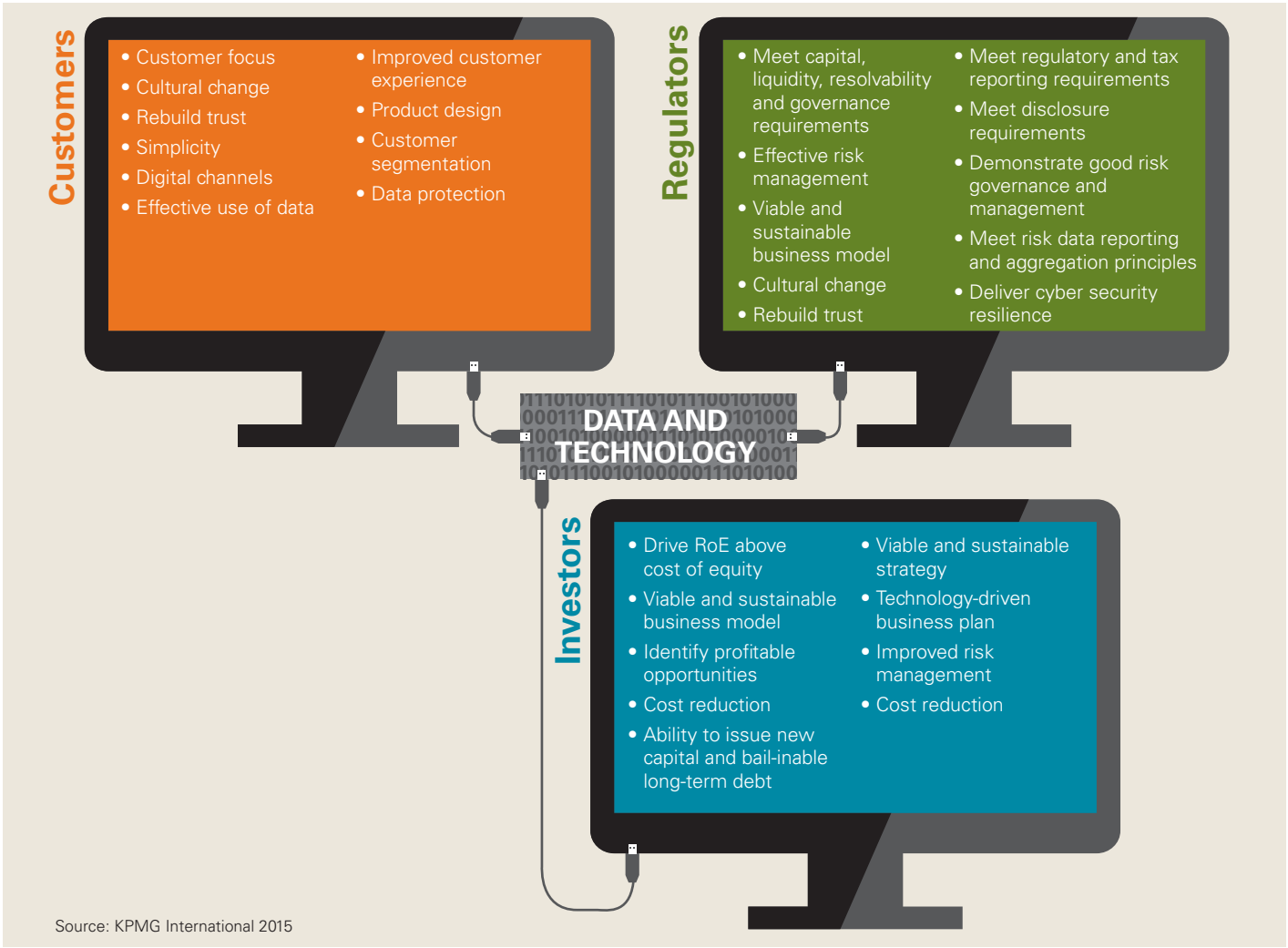
The regulatory reporting burden on banks has increased massively over the last few years, and is set to increase even further over the next few years. Increased regulatory requirements and more intensive supervision have driven a seemingly insatiable appetite for data among regulators – to monitor adherence to regulatory requirements; to support stress testing; to answer one-off information requests; to provide the raw materials for recovery and resolution planning; to open a lens on non-bank financial channels; and to access system-wide data for macro-prudential policy purposes.

In addition, regulators have focused increasingly on the **public disclosure of information** to enhance comparability, market discipline and market trading and price formation; on **risk data aggregation and reporting within banks**; and on alternative sources of data to underpin **revised standardised approaches to credit and market risk** that are more risk-based and less dependent on external credit ratings.

Finally under the regulatory heading, the various regulatory initiatives on **know your customer, sanctions, tax, data protection and the treatment of both retail and wholesale customers** all carry significant implications for data and technology, while the sharper spotlight on **off-shoring risk and cyber security and resilience** will surely be converted into further regulatory requirements on data and technology in due course.

This regulatory intervention raises **fundamental questions about the data and technology that the senior management of banks should be using to run their businesses**. In part the issue here is whether banks have the systems and data architecture required to meet regulatory requirements. But there is also an issue here about the widening gap between the internal models currently used by many banks for capital planning, pricing and risk management, and the new regulatory perspectives on how banks should be run, including regulatory constraints on the use of internal models to calculate risk weights.

What do banks need to do to meet stakeholders' demands?



Source: KPMG International 2015

Data

High quality data and data analytics are key to servicing customer needs, unlocking commercial value and supporting good risk governance.

Many banks could – and need to – improve customer experience through better use of data to design products and services, and to identify and meet customer needs more effectively. But there is also a regulatory question lurking here – will concerns about mis-selling, data privacy and cyber security lead regulators to constrain the extent to which banks are allowed to collect, store and analyse customer-specific 'big data'?

Data and data analytics can also unlock commercial value. Banks need to understand better the relative performance of their business activities in terms of viability, sustainability and resolvability; and thereby to develop new strategies and business models.

Data are also critical to effective risk governance. Banks cannot identify and monitor their risks effectively without high quality data and the upward reporting of meaningful management information.

All these uses of data require the accurate and timely recording of data, effective processes for the use of data, and clear governance and ownership of data and data processes.

Technology

Efficient and effective technology is key to meeting customer demands to access products and services though digital channels, reducing costs, maintaining and improving operational resilience, and supporting good data management and risk management.

Customers of banks are increasingly expecting a digital service that matches the best non-banking digital channels. Banks with the technological ability to deliver such services can gain a clear competitive advantage.

Technology is also one critical component to delivering cost reductions, or at least to avoiding the costs arising from a low level of operational resilience. Banks need to focus on the overall resilience of their provision of critical economic functions such as retail deposit-taking and payment and settlement systems.

Banks with multiple and fragmented IT systems, in particular where these have been outsourced, are exposed to falling seriously behind the game and failing to secure a viable and sustainable future.

These banks therefore need to develop a clear strategic vision, and a clear road map of how technology can drive improvements in customer service and risk management; how technology can – together with simpler business activities and simpler legal and operational structures – drive cost reductions; and how a governance framework and IT strategy can deliver operational resilience through high standards of service delivery, IT infrastructure, operational continuity and cyber security.

Banks need to overcome any lack of leadership, expertise and confidence to make the necessary changes. The cost of inaction will eventually exceed the cost of investing for the future, even during a sustained period of low returns.

Implications for banks

Banks face major – and costly – issues in responding to the regulatory and commercial pressures on data and technology. These issues can be grouped into five main areas.

Data capture, quality and integrity

Most fundamentally, many banks need to make further progress in improving the quality and harmonisation of their data. These banks face the very basic – but far from trivial – problem that the data required for improving customer experience, internal risk management, and internal and external reporting are simply not in place or are inaccurate.

Many banks currently hold and manage their data in silos, and report data from these silos. Data may be difficult to reconcile across systems, across business activities, across geographies, across legal entities, between the business and the second lines of defence (risk and compliance), and between regulatory reports and financial statements. This leads to duplication, delays in assembling both internal and external reports, inconsistencies and inaccuracies, and a need to rely on manual processes and work-arounds.

This compromises the ability of these banks to aggregate risk data quickly, accurately, and across all risk types, activities and geographies. As a result they face challenges in producing and using high quality management information as an input to high quality risk identification, measurement and monitoring, and high quality decision making at senior management and Board level.

Banks need a sustainable and robust data infrastructure from which to meet existing and prospective reporting requirements, and to respond to internal and external ad hoc information requests. Banks therefore need to focus on the standardisation of data held across banking groups, including the use of common definitions and common formats. Data can then more easily be subject to a 'single view', be centralised in terms of ownership, control and storage, and be aggregated for a variety of purposes.

Data analytics

Many banks also need to improve their data analytics capability. Banks need to extract more value from their data to become more customer-centric through a better understanding of customer needs and serving these customers more effectively, efficiently and profitability; to remain competitive with other banks and with actual and potential new entrants to banking markets; to identify emerging trends and issues more effectively; to enhance their ability to run stress tests; and to monitor trader behaviour and detect unauthorised trading and other suspicious activity.

Data governance

Data governance (at Board and senior management level) has moved up the agenda at many banks. This reflects both regulatory and commercial pressures. Issues here include the ownership and control of a bank's data, the governance of risk data aggregation and reporting, IT capabilities for data management and analysis, and assurance and attestation processes for the accuracy of data and reporting and for compliance with regulatory requirements.

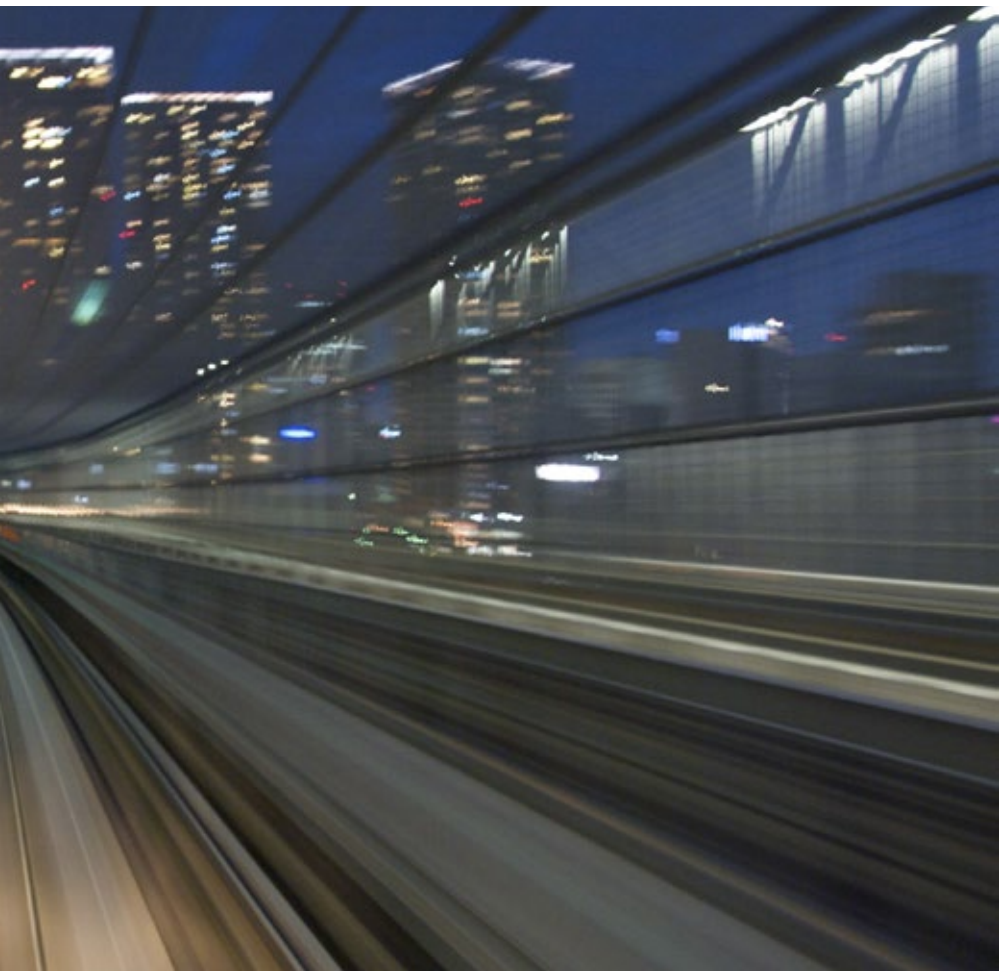
Some banks have responded to this by raising the profile of their Chief Information Officer, which in turn may be linked to the increasing emphasis being placed by regulators on the personal responsibility of senior managers. Indeed, the Bank of England has signaled that its Senior Manager Regime will include accountability for cyber security.

Many banks have initiated projects around various aspects of data quality, management, reporting and governance, but without being able to explain how improvements in data quality will be delivered; how data governance and data management work together; how they will move from expensive projects to business as usual; what the end state will look like; and how it will comply with the Basel Committee Principles on risk data aggregation and reporting.

Data protection and security

Many banks need to improve the security of their data and resilience against cyber attacks. In addition to various regulatory requirements on data protection and cyber security, banks should have a strong self-interest in implementing and maintaining strong standards for the protection of the data they hold on their customers, and for protecting themselves against cyber attacks.

One important aspect of this security is that data protection remains one of the few areas in which customers rate banks more highly than other service providers. At a time when the reputation of the banking sector is generally low, and customers are looking to banks to provide services increasingly through digital channels, this could be a key bridge towards banks regaining trust and reputation.



Technology

Many banks need to take major steps to improve their technology. In addition to deficiencies in the data, many banks lack the technology necessary to:

- Deliver effective and efficient data management. The number of data items is increasing rapidly, as is the importance of being able to report (internally and externally) and analyse these data;
- Improve risk management;
- Reduce costs through streamlining and efficiencies; and
- Meet the challenges of some incumbent banks, new entrant banks and non-bank technology-driven providers, who are all seeking to carve out profitable opportunities by using technology more efficiently and effectively for the provision of some banking services.

Many banks remain constrained by their disparate, fragmented, ageing and increasingly unreliable IT systems and infrastructures. Years of stitching together multiple discrete legacy systems of various vintages, of developing technology through a mixture of in-house, off-shored and outsourced routes, and of successive add-ons, work-arounds and manual interventions, have left these banks poorly placed to compete effectively.

The design and implementation of the necessary improvements may require large-scale and expensive projects to introduce a new IT infrastructure. These projects will need to be carefully prioritised during a period of resource and time constraints, and as banks also need to invest in meeting other regulatory and commercial pressures.

Regulatory pressures on banks

The data-related regulatory burden on banks is **no longer confined to the reporting of data to their national supervisors.** This aspect of regulatory pressures has increased massively over the last few years, but in addition:

- Newer entrants to the supervisory and regulatory arena – including the ECB, the European Supervisory Authorities, and national and EU banking union resolution and macro-prudential authorities – have all been formulating their own demands for data and other information from banks;
- Banks are being required to publish ever more information through Pillar 3 disclosures, and to report wholesale market trades and securities financing transactions;
- The proposed revisions to the standardised approach to credit risk will require all banks to collate and utilise data on the 'risk drivers' that will determine risk weights;
- The pressure on banks to improve their risk data aggregation and reporting is increasing, and is becoming a key element in supervisory assessments of banks' internal risk governance;
- Banks in the EU will face requirements to collate and publish data relating to simpler securitisations and on SMEs, as part of the development of the capital markets union (CMU);
- Pressures continue to mount on banks to improve their use of data and record-keeping in support of the fight against money laundering, terrorist financing and tax evasion by bank customers; and
- Various authorities are developing approaches that may eventually constrain banks in terms of data privacy, data storage, cyber security, and even the use of data to cross-sell products and services (especially to retail customers).

In response, banks need to:

- Anticipate these initiatives and their likely impact on data reporting requirements;
- Undertake an impact assessment of not only the individual initiatives but also the combined impact of these initiatives – and indeed the combined impact together with post-financial crisis data reporting requirements that have already been introduced;
- Consider the systems and quality controls that will need to be put in place to reduce the risk of reporting errors;
- Recognise the overlap of the process related and technical challenges of data reporting with the data and systems requirements under the Basel Committee's risk data aggregation and reporting principles. It should be beneficial for banks to achieve an early and close alignment of these projects, and to take into account not only technical overlaps but also organisational challenges such as the availability of resources and IT capacities;
- Align responses to regulatory data demands as far as possible with how the senior management of banks want to use data to run the bank; and
- Continue to develop consistent and flexible data sources to be able to meet ad hoc regulatory requests.

Regulatory pressures on banks' data and technology

Regulatory reporting

Last year's *Evolving Banking Regulation* highlighted the exponential growth in the amount and granularity of banks' regulatory reporting requirements. Each new regulation, and each new supervisory initiative brings with it additional reporting requirements. This in turn places burdens on banks in terms of the people, data capture, management and governance, IT systems and quality assurance processes necessary to support this reporting.

Looking back over the last year ….

Regulatory reporting requirements have increased substantially over the past year. The most significant data demands on banks in the EMA region have included:

COREP and FINREP went live in the EU in 2014. Banks were generally able to meet the more extensive reporting requirements, although some smaller banks struggled to meet the deadlines. Some banks have commented that their supervisors have raised fewer questions on these reported data than they had been expecting – which is perhaps a sign that the supervisors themselves have struggled to absorb and analyse the much expanded volume of reporting. Meanwhile, it is important for banks to recognise that COREP and FINREP are not set in stone – further reporting fields are being added in areas such as forbearance, asset encumbrance and the leverage ratio.

The **ECB's Comprehensive Assessment** exercise required major banks in the EU banking union area to produce and analyse a vast amount of data for the Asset Quality Review (AQR), while major banks across the EU were required to report detailed data as part of the EBA's 2014 stress testing exercise. Moreover, the ECB's AQR revealed structural weaknesses in some banks' data systems, and the ECB has already highlighted that data integrity is one thematic area it will be pursuing with banks during 2015.

The implementation of the **EU's Bank Recovery and Resolution Directive** in January 2015 has increased regulatory demands on banks to provide detailed information on their recovery plans, and to provide the extensive information base necessary for resolution authorities to construct resolution plans.

National legislation on **structural separation** and the evolution of the EU's proposed Regulation on structural measures – as outlined in Part Two of this year's *Evolving Banking Regulation* – have required major banks in some countries to provide detailed data on their trading activities and to consider how best they can police the boundaries being imposed on them by regulation.

The development of **macro-prudential authorities** – as described in Part One of this year's *Evolving Banking Regulation* – has been accompanied by increasing demands on banks to provide information to enable these authorities to analyse risks to financial stability. This has included data on the interconnectedness of banks to other banks and to other financial institutions (including the 'shadow banking' sector), and on the pattern of loan to value and debt service ratios relating to residential mortgage lending.

The first round of **country-by-country reporting** of profits and headcount data under CRD4 has been completed. In addition the Organisation for Economic Co-operation and Development (OECD) has set out a range of reporting requirements under its Base Erosion and Profit Shifting initiative, which will lead to significant additional reporting for tax purposes.

Looking ahead ….

Further demands on banks for data reporting will arise from a wide variety of regulatory initiatives, increasing the pressure on banks to respond to these initiatives while implementing the requirements that have already been finalised.

> "The development of macro-prudential authorities – as described in Part One of this year's *Evolving Banking Regulation* – has been accompanied by increasing demands on banks to provide information to enable these authorities to analyse risks to financial stability."

Regulatory reporting by major banks

A KPMG survey of 19 G-SIBs found that:[1]

- Surprisingly for such a data-intensive process, only 40 percent of the sample had an automation level above 75 percent for regulatory reporting; and a quarter had less than 50 percent automation coverage;
- Resourcing and competing priorities remained a constraint on further automation, thereby leaving many of these banks exposed to reporting errors and slow submission of regulatory returns;
- Nearly 80 percent of the sample had been subject to regulatory review or investigation of their RWA calculations in the last three years, with this figure rising to 94 percent for capital calculations;
- In response, 64 percent of the sample had put in place internal assurance processes on their RWA and capital calculations;
- However, only 56 percent of the sample were comfortable that their first line of defence reporting controls are fully documented and assessed; and
- Board oversight of regulatory reporting remains much less intensive than of financial statements.

[1]KPMG G-SIFI Benchmarking Survey 2015

> Pillar 3 of the Basel framework aims to increase transparency and confidence about a bank's exposure to risk and the overall adequacy of its regulatory capital, and thereby to promote market discipline.

International standards and initiatives

(i) Pillar 3 disclosures

The Basel Committee finalised in January 2015 the first phase of its review of Pillar 3 disclosures by banks. Pillar 3 of the Basel framework aims to increase transparency and confidence about a bank's exposure to risk and the overall adequacy of its regulatory capital, and thereby to promote market discipline.

From late 2016 banks will be required to publish an enhanced set of standard templates and other information in a less prescriptive format on:

- Movements in their overall risk weighted assets;
- Linkages between their financial statements and regulatory exposures;
- Credit risk, including credit risk mitigation, credit risk under the standardised and internal ratings-based approaches, and counterparty credit risk;
- Securitisation; and
- Market risk.

This will require banks to publish a greater volume and granularity of Pillar 3 disclosures, and in some cases on a more frequent (quarterly) basis.

Meanwhile, phase two of the Basel Committee's review will consider:

- Enhancements to reporting on other areas covered by the existing Pillar 3 framework, including operational risk and interest rate risk in the banking book;
- How best to consolidate all existing and proposed Pillar 3 disclosure requirements relating to the new post-financial crisis Basel Committee standards, including remuneration, the composition of capital, the leverage ratio, the liquidity coverage ratio and net stable funding ratio, and higher loss absorbency requirements on global systemically important banks;
- A standardised suite of resilience measures that could serve as early warning signs of distress, based on the indicators suggested in the Basel Committee's July 2013 discussion paper on balancing risk sensitivity, simplicity and comparability;
- Whether to require banks using internal ratings-based approaches for credit risk to disclose hypothetical capital requirements according to the proposed new standardised approach to credit risk (see below); and
- How best to implement the recommendations made by the Enhanced Disclosure Task Force (EDTF), a private sector initiative facilitated by the Financial Stability Board, which was established to improve banks' risk disclosures.

(ii) Revised standardised approaches

The Basel Committee's proposals on revised standardised approaches for credit, market and operational risk, and for a new capital floor to replace the 'Basel 1' floor (described in Part One of this year's *Evolving Banking Regulation*) will require all banks – including those using internal models to calculate capital requirements – to calculate their capital requirements under these new standardised approaches. For credit risk in particular this will require banks to collect and apply data on the proposed new 'risk drivers' for different types of credit exposure, including the revenues and leverage ratios of corporate borrowers; loan to value and debt service coverage ratios for residential mortgage lending; and the capital adequacy and asset quality ratios of bank counterparties.

(iii) Expected credit loss accounting

The implementation of IFRS 9 on expected credit loss accounting will place new demands on banks to collect, analyse and monitor data on their credit exposures.

The Basel Committee has issued a consultation paper on revised credit risk management principles relating to expected credit loss accounting, including data and system requirements on banks.

(iv) Stress testing

Stress testing by the EBA and national authorities has already increased the demands for data from major banks, and has required banks to demonstrate their ability to develop and apply their own stress testing scenarios that reflect the full range of their material business activities and risk exposures. This will increase further as stress tests are applied to more banks, and as these stress tests expand their focus to risks such as emerging market exposures, sovereign debt, and funding and liquidity.

The announcement by the Bank of England of the stress tests it will run in 2015 provides a good example of a shift in focus. The Bank of England will use a stress scenario that focuses more on global risks (weaker activity in China and the euro area) than domestic shocks; on deflation rather than inflationary shocks; and within the UK on bank exposures to the corporate rather than the household sector. The Bank of England will also apply a tougher and more elaborate traded risk scenario, including not only shocks to credit spreads and equity prices, but also the impact of further reductions in the liquidity of market positions and of counterparty defaults.

(v) Liquidity

Requests from supervisors for more detailed data from banks on their funding and liquidity, and on their sensitivity to bank-specific and market-wide stresses, are emerging as a result of the increasing role of funding and liquidity within stress testing, the implementation of the liquidity coverage ratio from January 2015, the prospective introduction of the net stable funding ratio from January 2018, and the increasing supervisory focus on liquidity within Pillar 2 evaluation.

(vi) Resolution

In addition to the vast array of information required on banks' critical functions, critical shared services and legal and operating structures required for the construction of resolution plans by the resolution authorities, one growing focus of some resolution authorities is on the need to be able to value a failing bank at the point at which it enters resolution. This in turn may lead to requirements on banks to increase their state of readiness for such an event by developing and applying valuation techniques that could be used in such circumstances.

(vii) Alternative channels of financing

Banks will be required to report more data on their exposures to and from alternative channels of financing as macro-prudential and other authorities develop their oversight of 'shadow banking'.

(viii) Tax

In the tax area, large amounts of customer data will have to be reported to the US Internal Revenue Service under the FATCA regime (with the first round of reporting due by 31 May 2015); and far more reporting of information on foreign domiciled customers to national tax authorities will be required under the provisions of the Common Reporting Standard (see box on page 12), to enable tax authorities to share more information with each other. This is in addition to the continuing upward pressure on banks to retain and report 'know your customer' information relating to anti-money laundering (AML) and terrorist financing.

Common Reporting Standard

More than 50 countries have signed up to the Common Reporting and Due Diligence Standard (CRS), which contains the reporting and due diligence standards that underpin the automatic exchange of financial account information.

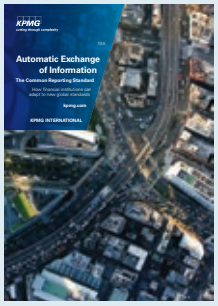
Under the CRS, banks and other financial institutions will be required to transmit financial data on their customers with a foreign tax domicile to their national tax authorities. National tax authorities will then forward the data to the tax authorities of the country where the customer is domiciled, so that they can check whether the customer's income on financial assets has been taxed correctly.

Most customer financial accounts and transactions are covered, although there are some exceptions, for example for some types of pension fund. Reportable accounts include accounts held by individuals and entities (which includes trusts and foundations – the CRS includes a requirement to look through passive entities to report on the individuals that ultimately control these entities). The CRS also describes the due diligence procedures that must be followed by financial institutions to identify reportable accounts.

The financial information to be reported with respect to reportable accounts includes all types of investment income (including interest, dividends, income from certain insurance contracts and other similar types of income), and also account balances and proceeds from the sale of financial assets.

Banks will therefore need to:

- Identify relevant customers, by checking the domicile for tax purposes of new customers (in most countries, from January 2016) and identifying this domicile from the existing information held on current customers;
- Identify relevant customers that benefit from trusts and other similar arrangements;
- Identify relevant accounts; and
- Report the necessary data to their national tax authority in defined formats.



Automatic Exchange of Information – The Common Reporting Standard

EU standards and initiatives

(i) Trade and transaction reporting

The demands on banks for trade and transactions reporting will increase significantly with the implementation of MiFIR and MiFID2 from January 2017. In essence, MiFIR extends the scope of the earlier MiFID1 to cover:

- almost all financial instruments (extended from equities and some equity exchange-traded derivatives under MiFID1);
- a wider range of trading venues (extended from MiFID1 to include organised trading facilities);
- non-EU branches of EU firms;
- three times as many data fields for each transaction (extended from MiFID1 to include the use of legal entity identifiers, the identification of both clients and end-clients, the time stamping of transactions, the identification of the traders and algorithms that make and execute an investment decision, and reporting flags for short-selling, commodity derivatives and waivers); and
- data storage requirements (extended from MiFID1 to include orders as well as transactions).

Meanwhile, MiFIR seeks to make it easier for commercial providers to produce consolidated data tapes, through more standardised reporting and data formats.

The European Securities and Markets Authority (ESMA) continues to develop technical standards under MiFIR. However, it remains unclear whether the European Commission and ESMA will be able to iron out all possible duplications and inconsistencies within MiFIR, and between MiFIR and other sets of requirements – the reporting of derivative trades under EMIR, the reporting of securities financing transactions (see below), and the reporting of wholesale energy transactions under the EU Regulation on Wholesale Energy Market Integrity and Transparency (REMIT).

The experience with transaction reporting in the UK suggests that banks find it difficult to report accurately, resulting in a long series of enforcement actions. The highest UK penalty to date (£13.3 million) for transaction reporting errors was imposed on Merrill Lynch International in April 2015 for failing to report 121,000 transactions and inaccurately reporting 35 million transactions between 2007 and 2014. ESMA intends to develop templates and protocols for transaction reporting that could reduce the number of errors.

(ii) Securities financing transactions

The proposed EU Regulation on the reporting of securities financing transactions (SFTs) requires the counterparties to such transactions to report them to an ESMA-registered trade repository no later than one working day after the transaction, and to keep records of their SFTs for at least 10 years. A counterparty includes financial institutions that are established in the EU, together with all their branches world-wide, and those established outside the EU if they undertake an SFT through a branch in the EU.

(iii) Supervisory evaluation

The EBA is calling for additional regulatory reporting by banks in a number of areas, including quarterly metrics relating to each of the risk areas identified in the EBA's guidelines on the supervisory review and evaluation process.

(iv) External assurance

Continuing supervisory concerns about the accuracy and reliability of regulatory returns are resulting in greater emphasis being placed on some form of external assurance. There are already some requirements for this in countries such as Germany, the Netherlands, Spain and Switzerland. In the UK, the accounting profession (through the ICAEW) has been asked by the Prudential Regulatory Authority to explore the options for enhanced external assurance. Most banks acknowledge the need to do more here, recognising that too much reliance is currently placed on multiple systems and manual adjustments when completing regulatory reports. But there are mixed views on the most appropriate way forward here – external assurance, internal audit or senior management attestation.

(v) Capital markets union

The development of an EU capital markets union will introduce new data and reporting demands on banks, including the collection, assembly and reporting of data to support simple high quality securitisations, and the collection and provision of information on SMEs to help them to raise funds from other banks and from non-bank channels of finance.

ECB initiatives

(i) Financial reporting

The ECB is establishing a comparable financial reporting system for all banks and banking groups within the banking union, by extending the requirement to provide financial information in the form of a FINREP report from parent companies that prepare IFRS consolidated financial statements to a wider range of groups and to large individual banks. In addition, smaller banks and banking groups will be required to report a scaled-down version of FINREP, thereby extending some version of FINREP across all banks (not just those directly supervised by the ECB) in the banking union (except for those with a waiver from COREP reporting). For some banks, this will increase significantly their financial reporting requirements.

The extension of full FINREP reporting to major non-IFRS groups will begin from the end of 2015, while the scaled-down FINREP for smaller 'significant' and 'less significant' groups and individual banks will be introduced from June 2016 and June 2017 respectively.

(ii) Loan data

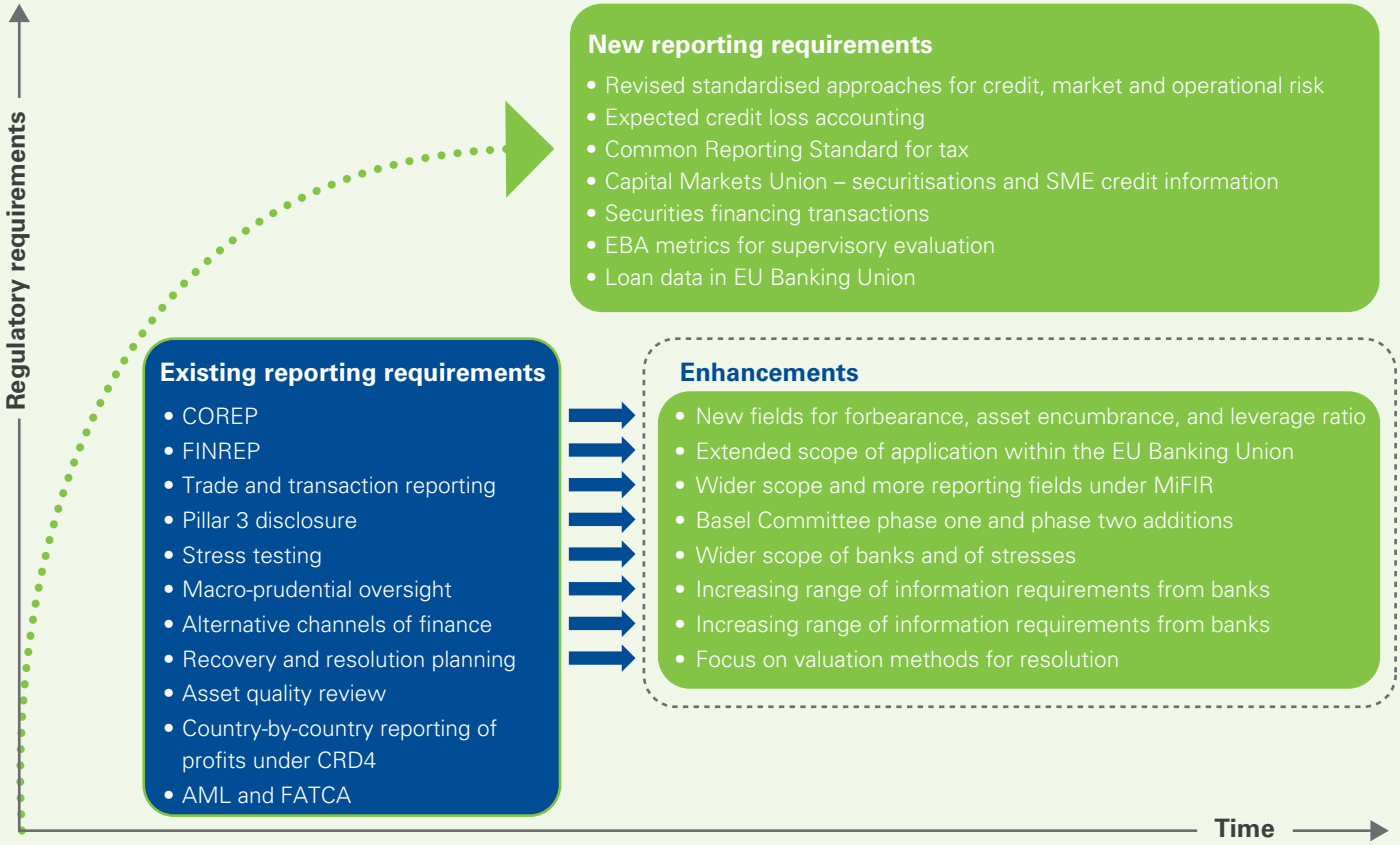
The ECB is also planning to collect and analyse detailed loan information from banking union area banks. Granular information covering numerous (around 100) attributes about individual loans will be collected, with an expected low cut-off threshold. The intention is that this will replace national credit databases, and will be phased in from 2017.

The ECB is investing in a complex infrastructure 'AnaCredit' to process and analyse these loan data, with the intention that this analysis can contribute to the ECB's overall statistical data, its micro-level supervision of individual banks, and its macro-prudential analysis of risks to financial stability.

At the micro level, the data will allow supervisors to see through to a 'glass bank' and to undertake more comprehensive analysis and consistency checks, following up and expanding the analysis undertaken last year under the AQR. The data will also facilitate more detailed analysis in areas such as the verification of banks' business models and the granting of loans to SMEs.

"The ECB is also planning to collect and analyse detailed loan information from banking union area banks."

Regulatory reporting



Source: KPMG International 2015

Risk data aggregation and reporting

The frustration of banking supervisors about the inability of major banks to aggregate their risk exposures quickly and accurately at both regulated entity and group level, for the purposes of both internal reporting and to meet information requests from supervisors, led to the development of the Basel Committee Principles on risk data aggregation and reporting (January 2013).

The Principles cover:

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 documentation, validation and robustness of these capabilities and processes;
- the design, build and maintenance of data architecture and IT infrastructure to support risk data aggregation capabilities and risk reporting practices both in normal times and during periods of stress.

The accuracy, integrity, completeness, timeliness and adaptability of aggregated risk data:

- the adequacy of the systems and controls that generate risk data and its aggregation; and
- the capability to adapt rapidly to changes in key risks and regulatory requirements.

The accuracy, comprehensiveness, clarity, usefulness, frequency and distribution of risk management reports, including to the board and senior management:

- procedures for monitoring the accuracy of data and model reliability;
- making good use of forward-looking assessments of risk; and
- reviewing the usefulness of risk management reports to senior management and the board, in particular as an input to properly-informed risk and business decisions.

The need for supervisors to review and evaluate a bank's compliance with these Principles, to take remedial action as necessary, and to cooperate across home and host supervisors.

G-SIBs are expected to meet these Principles by 2016, while D-SIBs should do so within three years of being designated as a D-SIB (it is left to national supervisors to undertake this designation). Supervisors may also apply the Principles to other banks on a proportionate basis. In Germany and Italy, the Principles have already been incorporated into legislative requirements on the minimum standards for all banks' risk management, and into the areas to be considered as part of the end-year audit.

Meanwhile, G-SIBs have been challenged to **self-assess themselves against these principles**. The Basel Committee has reported (in December 2013 and January 2015) the results of two such self-assessment exercises. **Nearly half the G-SIBs reported in the second exercise that they will be unable to comply fully with the Principles by the 2016 deadline,** and indeed the average ratings across the Principles had improved only marginally between the 2013 and 2014

self-assessments, in part because some banks had experienced delays in initiating or implementing large-scale IT infrastructure projects. This will inevitably lead to increased supervisory pressure on G-SIBs to prioritise achieving compliance with the Principles.

The three Principles with the lowest reported compliance related to **data aggregation**: data architecture and IT infrastructure, the accuracy and integrity of data, and adaptability. Nearly half of the G-SIBs reported material non-compliance with these Principles, and many reported that they were facing difficulties in establishing strong data aggregation processes, and were therefore having to resort to extensive manual workarounds. The banks also noted that even if their IT infrastructure was adequate in normal times, it would not be adequate in stressed conditions.

Under **data governance**, the most common weaknesses identified by the banks related to their need to improve their enterprise-wide governance framework; and to manage multiple large-scale projects related to risk data aggregation and reporting.

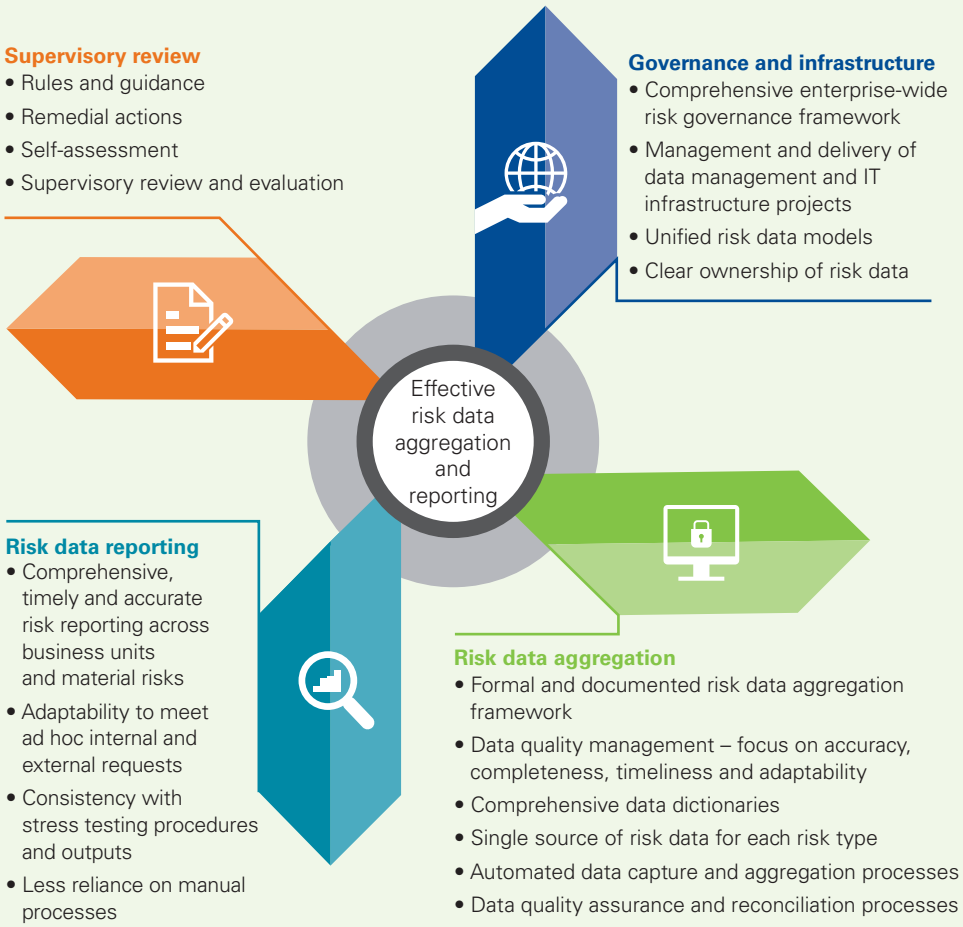
Banks self-assessed their highest compliance to be in relation to the **reporting of risk data**: report distribution, and the comprehensiveness, clarity and usefulness of reports. However, the Basel Committee has questioned how reliable and useful risk reports could be when the data within these reports and the processes to produce them have significant shortcomings.

The Basel Committee has concluded that banks need in particular to:

- **Upgrade significantly their risk IT systems and governance arrangements,** with an emphasis on formal and documented risk data aggregation frameworks, comprehensive data dictionaries that are used consistently by all group entities, comprehensive policy governing data quality controls, and controls at each stage of the life cycle of data;
- Improve their **risk data accuracy, completeness, timeliness and adaptability,** with less reliance on manual processes, and quality checks on risk data that are as robust as those supporting accounting data; and
- Generate relevant data on a **timely basis** to meet evolving internal and external risk reporting requirements.

In addition, the Basel Committee has called for **continued close supervisory oversight** of G-SIBs' progress in closing gaps with the aim of fully complying with the Principles, including the need for supervisors to engage more fully with banks' senior management, board of directors and internal audit on these issues, and to monitor more carefully banks' progress on IT architecture projects, reducing the use of manual systems, and quality controls.

The Basel Committee will continue to monitor G-SIBs' progress towards meeting the 2016 deadline.



Commercial pressures on banks

The pressures on banks do not arise only from regulatory reforms. As discussed in Part Two of *Evolving Banking Regulation*, banks also face an array of commercial pressures from the current and prospective economic environment, over-capacity in the banking sector, the emergence of challenger banks, and non-banks seeking to make inroads into profitable areas of banks' business activities.

Data and technology have become a mission critical element of banks' attempts to build a viable and sustainable strategy and business model. There are six key aspects to this:

- **Improving customer experience**
- **Exploiting technological advances**
- **Defending against competitors, including "digital disrupters"**
- **Enhancing risk management capabilities**
- **Reducing the cost base**
- **Countering the risks of cyber crime.**

Using data more effectively

Improving the customer experience is a key element in attempts by banks to rebuild trust and confidence in both retail and wholesale markets, and to increase their revenues and margins. Data, data analytics and technology can all play an important role here.

Banks hold **vast amounts of data**, but these data are usually held in multiple forms and places that do not communicate effectively with each other or with central data processing centres. Incompatible and inconsistent data sets increase the time and effort required for data aggregation and reconciliation. As a result, many banks find it difficult to gather and exploit data on their customers, and to take a single view of their customers based on robust, effective and operational systems.

These banks may therefore find it difficult to connect effectively with their customers; to identify profitable areas of business; and to drive simplification.

Indeed, the disconnect between banks and their customers may be widening, not least relative to rising customer expectations based on their experiences with firms in other industries who have performed better than the banking industry in using technological advances to understand their customers better and to communicate more effectively with them.

Once data are fully accessible, banks can use analytic tools to:

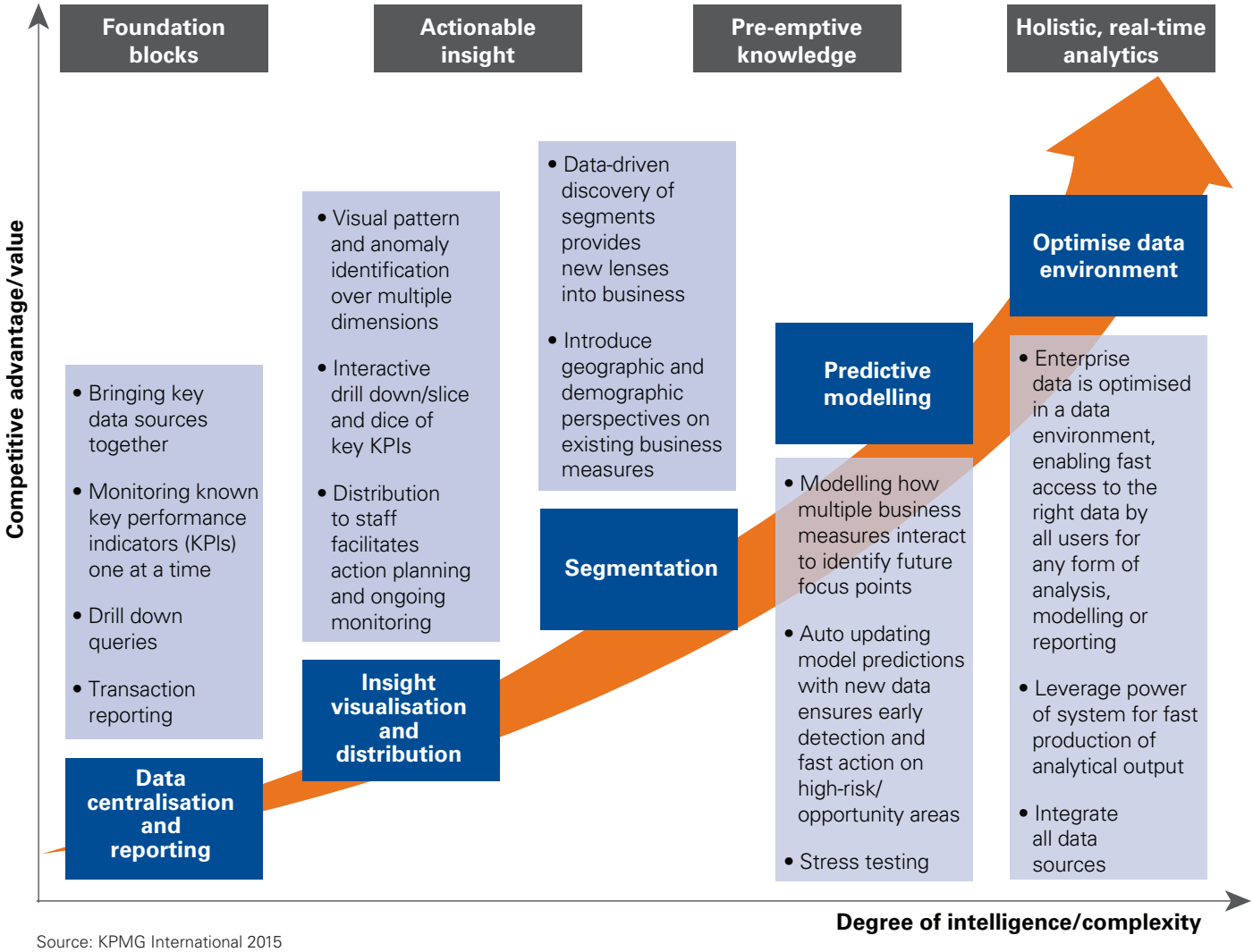
- Understand customer needs;
- Model customer behaviour;
- Enhance products and services and tailor them to customer needs;
- Segment the customer base (based for example on buying patterns, profitability, demographics and attitudes to risk);
- Make customer-specific product recommendations;
- Customise their marketing;
- Identify profitable opportunities across customers, products, legal entities, geographies and business lines;
- Identify emerging trends and issues;
- Enhance stress testing capabilities;
- Monitor trader behaviour and detect unauthorised trading and other suspicious activity;
- Improve key performance indicators and other management information; and
- Identify anomalies in how data are captured and reported.

Part of the answer for banks here is to make more effective use of **data analytics**. Banks need to extract more value from their data to become more customer-centric and to remain competitive with other banks and with actual and potential new entrants to banking markets. The real competitive advantage here will come from the successful integration and analysis of all sources of customer and market data.

Banks also need to think about what data they should be using to run the business. Despite all the emphasis of both banks and regulators on improved risk governance, regulation is driving a wedge between an internal models based approach to capital and liquidity planning and risk management, and regulatory requirements based on a revised standardised approach, the leverage ratio and the results of stress testing.

“Regulation is driving a wedge between an internal models based approach to capital and liquidity planning and risk management, and regulatory requirements based on a revised standardised approach, the leverage ratio and the results of stress testing.”

The data analytics maturity curve



Source: KPMG International 2015

Do you know how much is hidden beneath your IT Iceberg?

What is the IT Iceberg?

IT patch work
Legacy IT systems and contentious system upgrades

Old programming
Accumulation of numerous programming rules written over decades

Automatic IT systems
Processing transactions and issuing statements without human interaction and monitoring

'Corporate memory' loss
IT developers have left your company and nobody knows how to change the coding or make it compatible with new systems

Why we believe this is a major issue

A recent KPMG analysis[2] indicates that issues due to **legacy IT systems** are an emerging pattern in the financial services industry

Institutions are aware of this problem but are caught in **'analysis paralysis'** and don't know how to solve it

So, what impacts can it have on you?

Success
Technology dictates your future business success

Competition
No flexibility, not leveraging competitive advantage of data intelligence

Reputation
Reputational damage

Penalties
Risks of future fines and scrutiny

Customers
Loss of customer confidence leads to greater industry impact such as mass pay-offs

Why not leave the past behind?

Your improved IT system

Get ready for future business model practices

Enable your business to make decisions based on data analytics and intelligence

Close the chapter of issues and potential future fines

Stop mitigating risk, invest instead in future growth and economics of excellence

Make your legacy issues history

Source: KPMG in the UK, 2015 http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/pages/what-is-hidden-beneath-your-it-iceberg.aspx

[2]KPMG in the UK, 2015

High quality data and data processes also offer banks opportunities to **improve their risk management:**

- While the risk data aggregation and reporting focus of the Basel Committee has been primarily on prudential risks to the capital and liquidity of a bank, a similar issue arises with respect to business conduct – banks may be unable effectively to identify and to address mis-selling or other conduct failings if their data on sales of similar products or transactions are held in different forms across different parts of the bank;
- Data and management information can be used to support personal accountability for business performance and risk management, by providing a clear line of sight on outcomes relating to individual responsibilities; and
- Introducing automated smart systems may provide at least part of the solution to a number of AML, tax and trading concerns, and may provide scope to transform compliance monitoring.

Technology: from fragmentation to next generation

Even if banks begin to place more value on data and invest more in data analytics, many of them will remain **constrained by their IT systems and infrastructures**. These are typically disparate, fragmented, ageing and increasingly unreliable. They reflect the stitching together of multiple discrete legacy systems of various vintages during earlier periods of rapid expansion, mergers and acquisitions, and entry into new areas of business; and multiple provenances (in-house developments, off-shored development and fully outsourced), successive add-ons, extensions, work-arounds and manual interventions.

Banks have spent significant sums investing in and maintaining their data and IT systems, and many have made progress in stripping out multiple systems, but there is still a long way to go here. Many senior management teams remain frustrated by the limitations their data and systems place on them, creating inflexibility and slowing the pace of change within the organisation.

The **IT infrastructure of many banks requires immediate and expensive attention** before it becomes wholly unsustainable, let alone capable of facilitating automation and innovation; effectively supporting banks' target distribution channels; enabling banks to utilise data and technology as key competitive differentiators; and delivering effective cyber security resilience.

Many banks therefore need to **re-think fundamentally their IT systems and infrastructure**, and indeed to consider how they can become a technology-driven, not just technology-supported, bank. Legacy systems need to be replaced with a **single structure and operating model**, with an emphasis on standardised and simple approaches that facilitate internal data management, external reporting, innovation and automation; that are agile, robust and resilient; and that deliver a core set of platforms that are used by all channels – payments, customers, finance and risk – in a coherent and consistent way.

> Regulatory reporting and risk management requirements are already crowding out other technology projects.

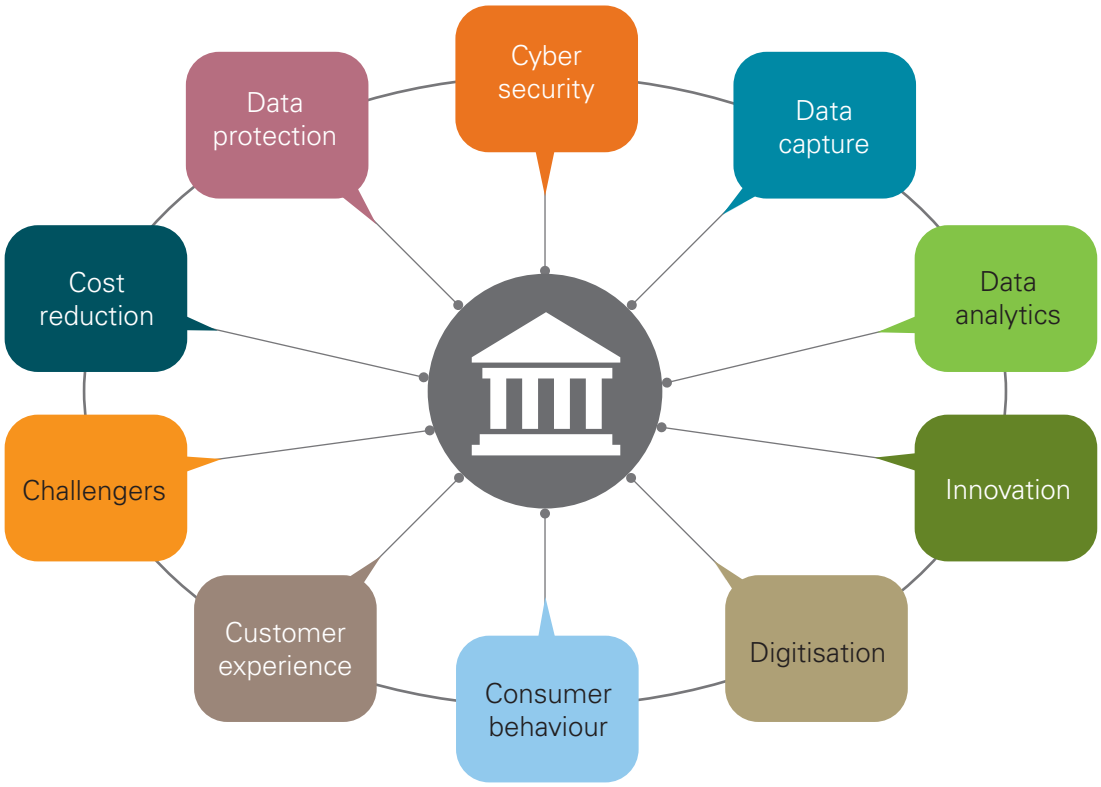
Meanwhile, harnessing technological advances could enable banks to **reduce costs** by:

- Streamlining their operations, reducing operating costs and increasing efficiency – in particular if technology and data management are capable of being scaled up and extended across business activities and geographies;
- Introducing greater industrialisation of processes in order to simplify, standardise and consolidate operations and thereby to reduce complexity and enhance customer service; and
- Reducing the costs – be they financial, regulatory or reputational – that emerge eventually from poor data and technology that in turn facilitate bad decision-making and inappropriate behaviours.

However, banks **face difficult choices** here:

- The up-front costs of technology projects arise at a time when banks' profitability is weak and pressures for cost reduction are strong;
- Regulatory reporting and risk management requirements – in addition to the costs and practicalities of meeting other regulatory initiatives (including, for some large European banking groups, legal entity rationalisation and meeting US requirements to establish an intermediate holding company and participate in CCAR) – are already crowding out other technology and data projects; and
- Banks need to decide how much change to introduce – shortcomings need to addressed, but the search for perfection raises the spectre of costs exceeding benefits.

Commercial pressures on banks' data and technology



Challenges: new channels and new competitors

The behaviours of bank customers are changing, with increasing use by customers of a multiplicity of new digital channels and applications, albeit alongside the continuing use of existing physical and digital channels such as bank branches and internet banking; new payment channels; and even new currencies such as Bitcoin.

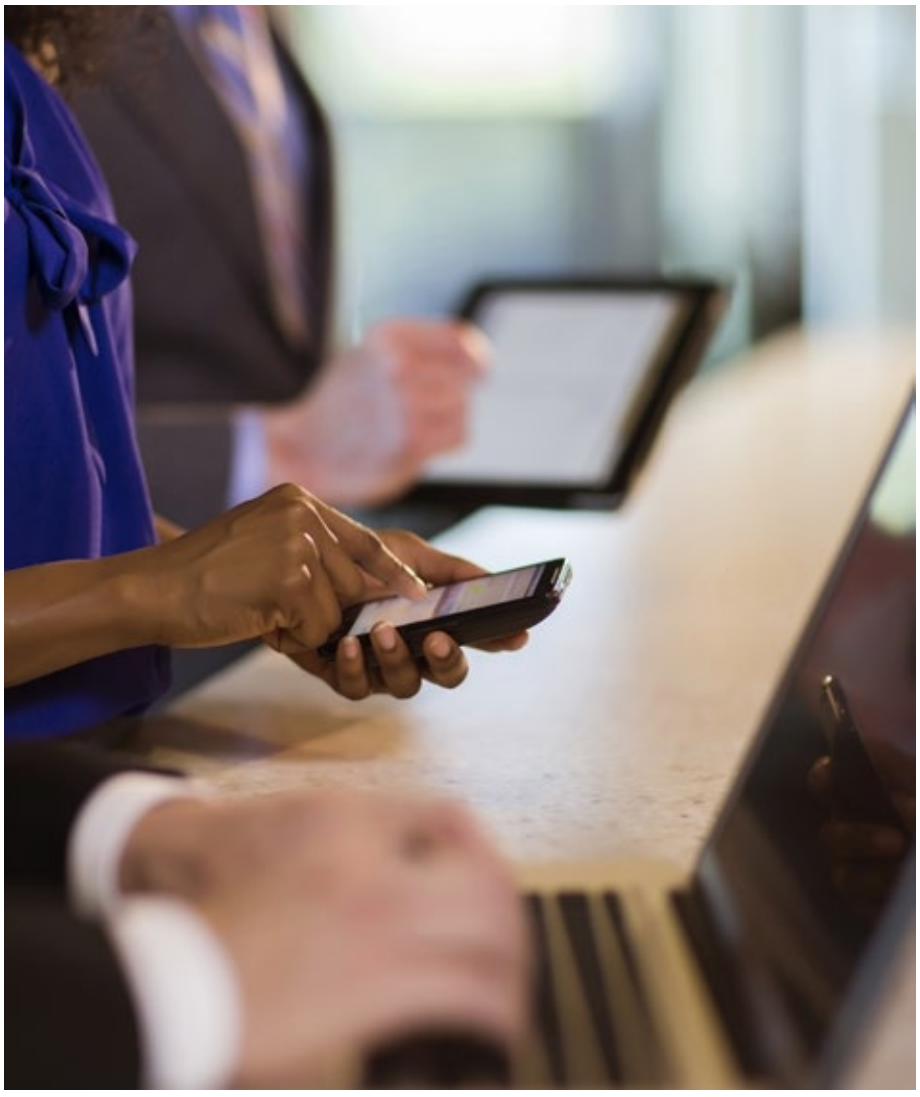
Banks in turn need to choose how to respond to this – they have a choice as to the balance between branches and digital channels, recognising that branches still have potential value in the personal contact they provide, and within digital between offering customer services across all available channels or specialising in a narrower range.

But wherever banks locate themselves on this spectrum the pressure from their customers is to offer a seamless and integrated service that is much the same wherever customers interface with their bank. Customers expect these new channels to work as quickly, efficiently and seamlessly as the best non-banking digital channels.

Banks face **challenges from new entrant banks** without all the legacy baggage of many existing banks – and indeed from some incumbent banks offering high standards of customer service through various channels. These challengers are seeking to compete by taking a more customer-oriented approach supported by the effective use of data and technology.

Banks also face **challenges from non-bank technology-driven providers** seeking to enter markets for simpler and more standardised (rather than knowledge-intensive) financial services, where there are opportunities to exploit technology and data-handling in areas where incumbent banks make large profits, or are relatively inefficient, or do not provide sufficiently high standards of customer service. This is often referred to as 'digital disruption', and while in practice not all of these challenges are digitally-driven they do all provide scope for new waves of innovation. These simpler and more standardised services include:

- Digital payment solutions – such as paying through a mobile phone or other electronic wallet without the need for cash or cards;
- Digital information services;
- Payment processing – a huge industry that generates large amounts of income though



> Banks can also seek to harness their strong existing customer relationships, their depth of data about their customers, and their integrated product and service offerings.

customer transaction charges, merchant fees and holding interest-free balances, and provides a potentially valuable source of information on customer purchases and money transfers;

- Automated financing – such as peer-to-peer 'market place' lending to SMEs, increasingly funded by institutional investors in addition to individuals;
- Digital currencies; and
- Automated advisory and securities trading services.

Clearly these challenges are a threat to incumbent banks, initially by nibbling away at the profitability of some business activities and potentially by replacing the banks as the primary provider of some services.

However, **there are also opportunities for established banks here**. Banks do not need to be a first-mover in technological change – they can potentially copy or adapt successful innovations.

For example, banks can use new channels, including social media as well as the provision of banking services, to connect better with existing and new customers. And banks can exploit innovation and technological progress to offer their customers an enhanced service – many banks have already improved their digital offerings to offer a more seamless customer experience across different channels; some are at the early stages of offering customers authentication based on voice or physical recognition, greater customer management of credit and payment cards, and alternative digital accounts and currencies; and some banks are looking to extend digital opportunities to a broader range of customers, for example through digital channels for private banking and asset management.

In addition, banks can potentially use new digital channels as part of the process of rebuilding customer satisfaction, trust and loyalty. They have a competitive advantage from their generally better record on security breaches than some of their major competitors for payment services. Indeed, despite the overall lack of trust in banks, and customer concerns over the ownership, security and privacy of their data, personal customers seem to trust their banks more than other non-bank players for the provision of digital services.

Banks can also seek to harness their strong existing customer relationships, their depth of data about their customers, and their integrated product and service offerings. New entrant banks often restrict themselves to a niche area of business, while most non-bank entrants are keen to steer clear of products and services that would require them to be regulated as banks. Banks can establish their own 'market place' lending platforms, and integrate social network and other digital sources of information about potential borrowers into their existing credit risk assessment processes.

The changing world of money

The game changers

Customer experience: some surprising results

A KPMG International survey in late 2013 of 5,000 consumers of their experiences of a sample of 160 organisations across sectors (banks, life insurers, general insurers, utilities and e-retailers) and across five countries found that:

- E-retailers had the highest scores for customer experience;
- Banks provided the second highest levels of customer satisfaction, ahead of general insurers, life insurers and utilities. Banks performed most strongly in meeting customer expectations where they had invested in operational excellence, security and technology. Australian and German banks scored most highly among the banks, with UK banks scoring the lowest (behind banks in the US and China);
- The most important areas for customers of banks were value for money (perhaps in part because the survey was conducted at a time of low deposit and savings rates) and the ability to interact with honest, trustworthy staff – which suggests that banks should not be investing solely in technology and digital offerings to improve customer experience; and
- There is a wide gap between how importantly customers of banks rate these two most important areas and the performance of banks in these two areas.

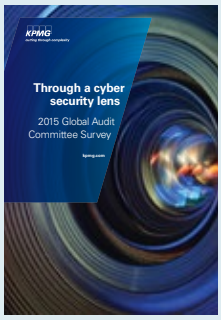
Customer Experience Barometer

Meanwhile, **regulators have their own concerns**, which complicate banks' strategic choices.

National regulators have already taken different approaches to the regulatory classification of new entrants to banking markets such as payment providers and peer-to-peer lenders, with some countries keen to regulate these new entrants as banks rather than as electronic money institutions or lending platforms. Subjecting new entrants to regulation will erode at least part of their competitive advantage over incumbent banks.

National regulators are also likely to differ in the extent of their concerns over banks potentially using data and technology for the inappropriate cross-selling and marketing of products and services (rather than for what regulators would view as the appropriate servicing of customer needs with suitable products and services); concerns over the security and privacy of customer data; and concerns over the adequacy of banks' data systems and data modelling.

National regulators will also influence the competitive landscape through their approaches to the acceptance of digital recognition for account access and know your customer purposes, and to the online availability of credit bureau information on individuals and companies.



Through a cyber security lens

Cyber security

The risks posed by cyber security attacks are moving rapidly up the corporate agenda, particularly in banks and other financial institutions. Boards, Risk Committees and Audit Committees are spending more time on cyber security risks.

KPMG's 2015 global audit committee survey showed that cyber security is one of the top three risks in 16 percent of the global sample of more than 1,500 firms; 40 percent of audit committee members thought that they should be spending more time on cyber security; and 41 percent were concerned that the information they received on cyber security needed improvement.

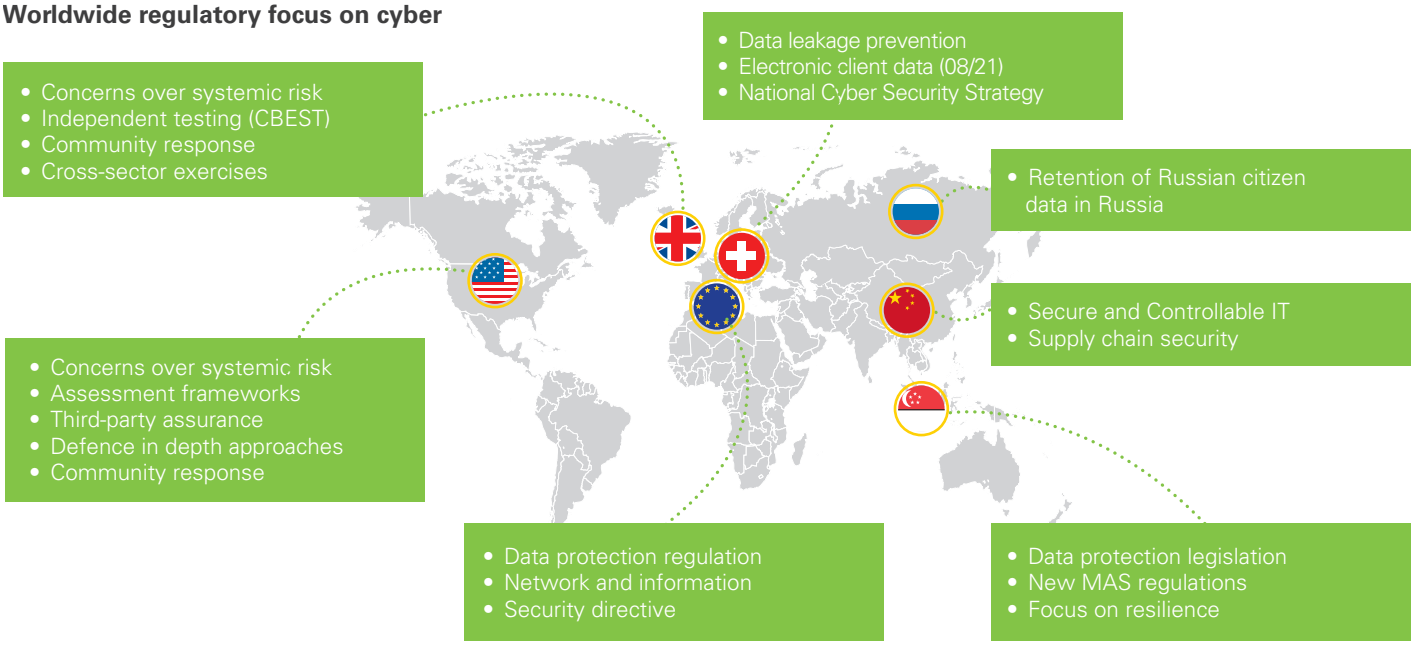
Banks are an attractive target for cyber attacks, because of their key role in payment and settlement systems, the amount of sensitive customer information they hold, and the potential adverse impact of interfering with the smooth functioning of banking services.

There have been a growing number of cyber attacks on banks, including:

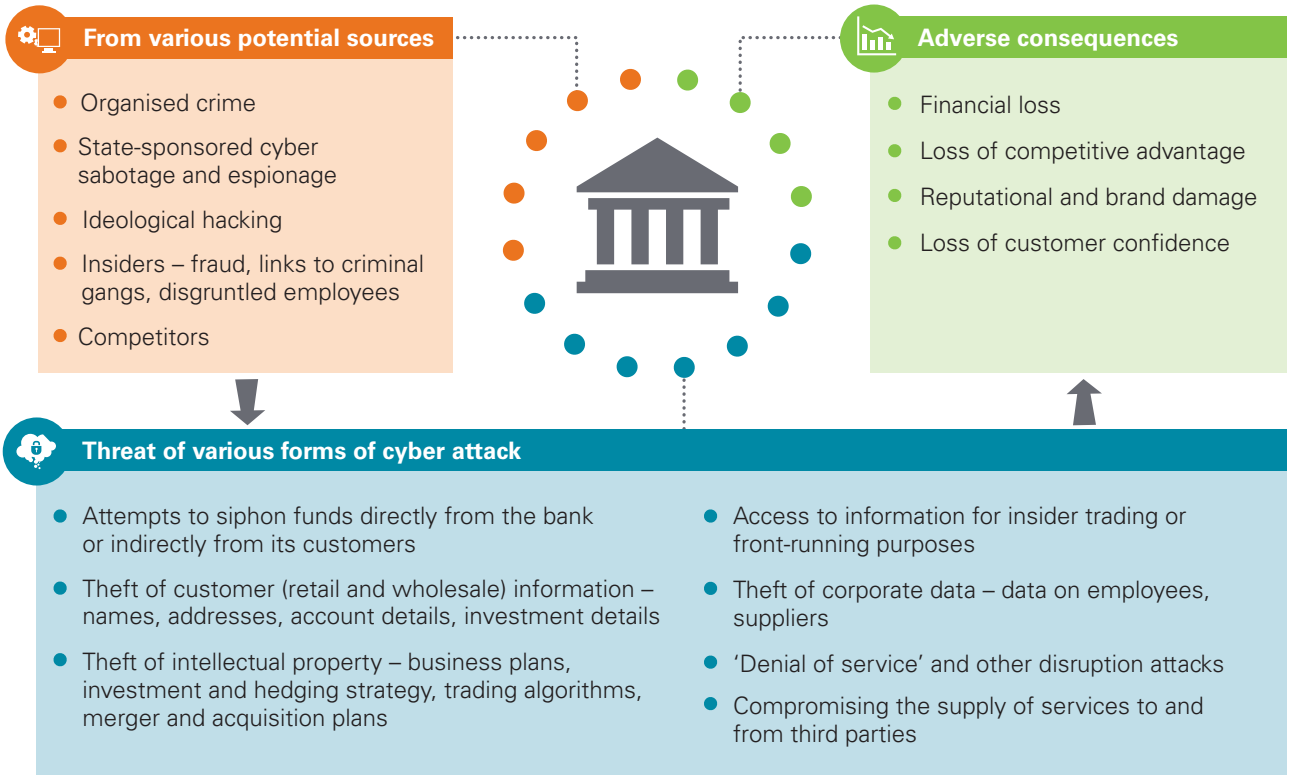
- Denial of service attacks, including on banks in Estonia in April/May 2007, some major US banks in September 2012 and UK banks in October 2012;
- The Carbanak advanced persistent threat attack on banks' internal systems and controls during 2013 and 2014 to facilitate fraudulent fund transfers;
- The 'Dyre Wolf' phising attack on corporate customers of banks; and
- A major US bank announced in August 2014 that a cyber attack had compromised data on 76 million households and 7 million small firms. No money was stolen from these customers, but access was gained to some account information.

Meanwhile, banks are exposing themselves to greater cyber security risks through measures intended to improve their efficiency and effectiveness. Banks are making greater use of technology to reduce costs; opening up their IT systems to a wide range of access routes as part of moves to improve customer service;

Worldwide regulatory focus on cyber



Nature of the threat to banks



holding a wider set of information on their customers (in part in response to increasingly onerous regulatory 'know your customer' requirements); and outsourcing IT development and IT services, customer data handling and storage, and internal systems such as payroll, office maintenance and security.

Cyber security is also moving up regulatory and government agendas. Market-wide simulation exercises have been conducted in the US and the UK to test the resilience of banks and critical market infrastructure in the event of a cyber attack; the ECB is undertaking a thematic review (initially mostly fact-finding) of banks' cyber security threats and precautions; and governments have become increasingly concerned about the threats to both their own interests and the critical economic functions run by utilities, banks and other companies.

Cyber security – implications for banks

As with other aspects of data and technology, a successful approach to cyber security can offer banks a competitive advantage by enabling them to maintain and improve the trust and confidence of their stakeholders, and to implement efficient and effective technology and data management.

Banks need to develop their mitigation of cyber security risks in four main ways.

First, banks need to recognise that **cyber security is not simply a technology issue**. As with other major high level risks, bank boards – and their risk and audit committees – and senior management need to make cyber security a priority issue in terms of managing risks to the business; assessing the extent to which business objectives expose a bank to

cyber security threats; seeking assurance that cyber security risk has been properly assessed and is being managed appropriately; identifying and gathering information of the threat; assessing the ability of existing systems and controls to deal with it; and acting strategically and tactically to counter the threat.

Second, banks need to **increase their resilience to cyber attacks**. This will require investment in a number of areas that sound relatively basic but which can be difficult and complex to deliver effectively:

Technology – building firewalls and other security features, and monitoring and detecting cyber attacks and security breaches;

People – security awareness (training and understanding) of a bank's staff, security policies for access to data and systems, the testing of the effectiveness of these policies in practice, and the retention of critical skills that are in relatively short supply;

Internal processes – the security requirements built into key internal processes; and the potential additional cyber security risks arising from entering new markets, developing new products and services, and utilising new technology such as trading platforms, internet banking and data warehouses;

Third party vulnerabilities – contracts with third parties should cover not just pre-contract due diligence about supplier security but also post-contract security audits. There are questions about the security of usage, storage and security of data at all points in the 'supply chain'. Banks need to understand who their suppliers are and what data these suppliers hold or have access to. Protecting the perimeter is not sufficient – third party suppliers, joint ventures and bank customers also have some degree of access to a bank's data and systems;

Threat intelligence – keeping up to date with the evolving nature of cyber security threats. Some banks are investing heavily in in-house capabilities to assess the threats; to undertake internal and external testing; and to identify possible preventative measures; and

Responsiveness – the speed and agility of response when cyber security breaches do arise, the subsequent learning of lessons and the adaptation of systems and controls, and the handling of any issues for reputation management.

Banks are already spending large amounts on cyber security. Until recently this was usually based on assessments using the US National Institute of Standards and Technology (NIST) Cyber Security Framework, a set of voluntary standards designed for critical infrastructure companies to use in developing a comprehensive cyber security programme.

More recently, however, the NIST framework has been incorporated into the Federal Financial Institutions Examination Council (FFIEC) Cyber Security Assessment Tool. This assessment tool comprises two parts:

Evaluation of Inherent Risk Profile – the inherent risk arising from a firm's technologies, connections with third parties, delivery channels, products, organisational structure and external threats.

Evaluation of Cyber Security Maturity – the extent to which a firm's practices, processes and behaviours can support cyber security preparedness across five domains.

01 Cyber risk management and oversight

Quality and effectiveness of governance, risk management, resources, training and culture.

02 Threat intelligence and collaboration

Monitor and analyse threat intelligence, share information.

03 Cyber security controls

Effectiveness of preventative, detective and corrective controls, processes and procedures.

04 External dependencies

Nature of third party connections, oversight and relationship management.

05 Cyber incident management and resilience

Planning and strategy for incidents; detection, response and mitigation processes and procedures; escalation and reporting.

Third, banks need to **take a risk-based approach**, assessing where the risk is greatest, what key critical systems, information and data assets are most in need of protection, and what actions need to be taken to protect corporate value.

Fourth, banks – together with other companies and national governments and government agencies – need to **take a collective, coordinated and global approach** to many aspects of cyber security. They need to share intelligence and to work together to counter cyber security threats. The most recent UK 'Waking Shark II' and US 'Quantum Dawn 2' resilience exercises both concluded that although progress had been made in various respects since previous exercises, there was room for improvement in terms of determining whether cyber attacks are bank-specific or more systemic in nature; creating a single co-ordination body from industry to manage communications during an incident; and improving co-ordination across regulators and governments, both nationally and across countries.

However, such co-ordination is difficult – banks may be unwilling to share information, while governments and regulators have taken different approaches to cyber security. There are differences across countries in the nature and extent of any government-led strategy to tackle cyber crime; to make the country more resilient to cyber attacks; to exploit knowledge, skills and capability to underpin a collective approach to cyber security; and to designate banking as a critical economic function.

There may also be scope for insurers to play a role in driving up standards of resilience, but insurance against cyber risks is currently at a relatively low level.

Cyber security regulation and supervision

The regulatory and supervisory landscape for cyber security is characterised by many of the same features as those arising elsewhere in the financial regulation universe – fragmented regulatory approaches across countries; pressures for both 'localisation' and extra-territoriality in the application of legislation and regulatory rules; and a somewhat uneasy balance between micro-prudential measures intended to increase the safety and soundness of individual banks, macro-prudential measures intended to protect against the systemic risks inherent in the 'cyber eco-system', and data protection measures.

There are five main strands to this landscape.

First, **collective and firm-specific resilience exercises**. In addition to the US and UK system-wide resilience exercises discussed above, the UK has led the way in 'ethical hacking' – live testing of the resilience of individual banks to cyber attacks undertaken by a group of experts acting on behalf of the regulatory authorities. This direct testing of cyber security (including the ability of banks to detect and respond to cyber attacks) has jumped ahead of the more traditional approach to reviewing a bank's control framework. Other countries may follow this lead.

Second, regulatory authorities are at an early stage in **developing rules and guidance** aimed at increasing the resilience of banks to withstand cyber attacks. This has always been covered at a high level through requirements on banks to have adequate systems and controls, but some regulatory authorities are looking to supplement this with more specific rules and guidance relating specifically to cyber security.

In the EU, the European Commission proposed in 2013 a Network and Information Security Directive, with the objectives of:

- Developing a stronger culture of risk management, with firms operating in critical sectors and public administration adopting appropriate measures to ensure network and information security;

- Establishing national competent authorities for network and information security; and
- Coordinated information exchange, detection and response at an EU level.

This Directive is expected to be agreed in 2015 and implemented by 2017.

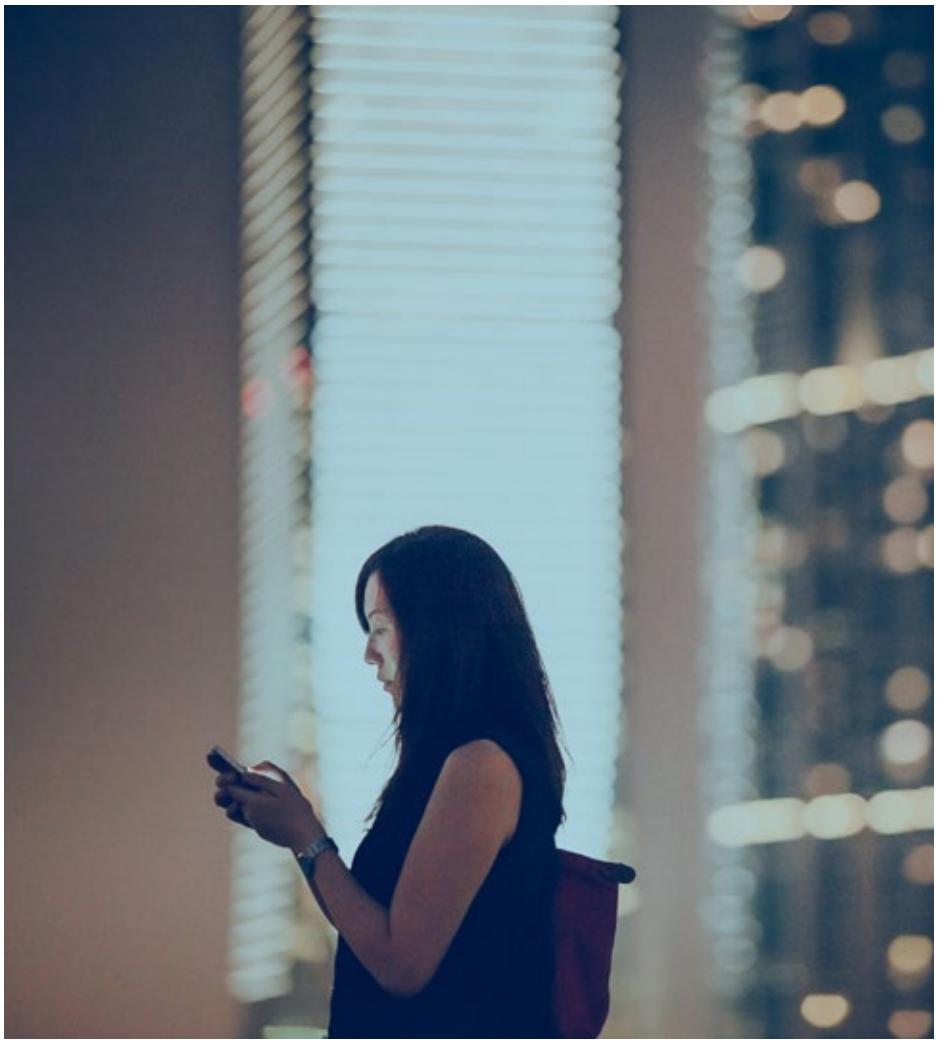
Third, **disclosure requirements**. Some countries are becoming much stricter in their requirements on banks to report cyber attacks to the regulatory authorities, and to report data privacy breaches to the relevant customers.

Fourth, **greater supervisory intensity.** Even where new rules and regulations have not been introduced, supervisors are stepping up their interest in banks' cyber risk policies. This includes supervisory interest in the extent of Board and senior management awareness, understanding and management of cyber risks; banks' ability to detect, report and respond to breaches; and banks' awareness of the risks posed by third parties with access to banks' systems and data.

Fifth, **data protection**. There are no internationally agreed standards for data protection, leaving the US and the EU to develop their own national and regional versions. In the EU this takes the form of the long-running attempts to introduce a new Data Protection Regulation and Directive, not least in order to update the existing Directive (which dates back to 1995) to reflect the shift from paper-based information to the world of the internet and online data collection and storage, and the much greater volumes of personal information that are now collected and stored.

Proposals from the European Commission (first put forward in January 2012) are based on the generally tougher approach in the EU to limiting the ability of firms (and governments) to record, store and distribute information on individuals. They include:

- A more consistent set of EU-wide rules (through the use of a Regulation), to limit the scope for national interpretations;
- A new EU-wide supervisory authority to settle disputes among national authorities;
- Enhanced rights for individuals to access and correct personal data held about them, and to be informed if data security is breached;
- Obligations on firms – both the owner of the data and any separate data processor or storage facility – to protect personal data, including adequate security protection over personal data;
- Tougher sanctions for breaches of data privacy requirements; and
- Limits on the storage of data outside the EU unless robust data protection standards are in place. This could limit the ability of non-EU firms to transfer customer data back to their home countries, and require global firms to operate multiple data centres.



KPMG Alliances and acquisitions

To meet the needs of clients on the complex, dynamic areas of cyber security and data and analytics, KPMG member firms have developed strategic alliances with a number of leading organizations around the globe in order to deliver leading service to clients. Some of the leading organizations that we have teamed with include…

UK

McLaren

Our Alliance with McLaren Technology Group is helping clients achieve break-through performance improvements, By combining KPMG's deep industry knowledge and operational experience, with McLaren's predictive analytics, simulation and high performance decision support, we're able to tackle complex operational challenges in a unique way. Our jointly developed technology, collaborative way of working and commitment to continuous improvement can be applied in many different ways: it could improve the efficiency of your mobile workforce by 30 percent, increase the productivity of your manufacturing operation by 50 percent, or achieve transformational enhancements to your supply chain to improve your customer experience.

Nunwood

KPMG acquired customer experience consultancy, Nunwood, that brings KPMG an in-depth customer experience management programme. Nunwood has a highly-respected annual brand benchmarking survey, the Customer Experience Excellence Centre; and a proprietary technology solution called Fizz, which measures customer interactions and allows companies to respond in real-time to customer data.

Spain

ADN

KPMG in Spain has acquired ADN, Spain's leading digital strategy advisory firm, into the firm's Management Consulting practice, strengthening KPMG's Strategy, Transformation and Data & Analytics capabilities.

Zink Security

KPMG in Spain acquired Zink Securities, a technology company specializing in information security and ethical hacking services. This acquisition allows KPMG to investigate and monitor events, information leaks, relationships between people, groups, entities etc. through information available on social networks, forums, blogs, news sites and deep web, to assist companies in monitoring, analysing and managing the mass of information generated daily.

Global

Cynergy

KPMG Cynergy is leading our digital experience design capability. Originally based out of the US, they deliver innovative customer/enterprise experience solutions, using a unique motivational design methodology and an agile collaborative approach to deliver technology and platform agnostic digital solutions.

Abbreviations

AML	Anti-Money Laundering
AQR	Asset Quality Review
CCAR	Comprehensive Capital Analysis and Review
CMU	Capital Markets Union
COREP	Common Reporting
CRD4	Fourth Capital Requirements Directive
CRS	Common Reporting and Due Diligence Standard
D-SIB	Domestic Systemically Important Bank
EBA	European Banking Authority
ECB	European Central Bank
EDTF	Enhanced Disclosure Task Force
EMA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
ESMA	European Securities and Markets Authority
EU	European Union
FATCA	Foreign Account Tax Compliance Act
FFIEC	Federal Financial Institutions Examination Council
FINREP	Financial Reporting
G-SIB	Global Systemically Important Bank
ICAEW	Institute of Chartered Accountants in England and Wales
IFRS	International Financial Reporting Standards
KPI	Key Performance Indicator
MAS	Monetary Authority of Singapore
MiFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
REMIT	Regulation on Wholesale Energy Market Integrity and Transparency
RWA	Risk Weighted Asset
SFT	Securities Financing Transaction
SME	Small and Medium Enterprises

Contact us

Jeremy Anderson
Chairman Global Financial Services
KPMG
T: +44 20 7311 5800
E: jeremy.anderson@kpmg.co.uk

Bill Michael
EMA Head of Financial Services
KPMG in the UK
T: + 44 20 7311 5292
E: bill.michael@kpmg.co.uk

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

Clive Briault
Senior Adviser, Financial Services
Regulatory Centre of Excellence
EMA region
T: + 44 20 7694 8399
E: clive.briault@kpmg.co.uk

Andrew Davidson
Director, Regulatory Centre of Excellence
EMA region
KPMG in the UK
T: +44 20 7694 2242
E: andrew.davidson@kpmg.co.uk

George Quigley
Partner, Information Protection and Business Resilience
KPMG in the UK
T: +44 (0) 20 7311 5603
E: george.quigley@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
Principal, Financial Services
Regulatory Center of Excellence
ASPAC region
KPMG China
T: +852 2826 7283
E: simon.topping@kpmg.com

fsregulation@kpmg.co.uk

www.kpmg.com/regulatorychallenges

kpmg.com/socialmedia

kpmg.com/app

Designed by Evalueserve.
Publication name: Evolving Banking Regulation – Part three: Data and technology: The regulatory and business challenges
Publication number: 132588-G