KPMG
cutting through complexity

Evolving Banking Regulation Part Four

Governance: from expectations to delivery

November 2015

kpmg.com

KPMG INTERNATIONAL

Contents

Executive summary 4

Banks: Further progress needed 8

International standard-setting 12

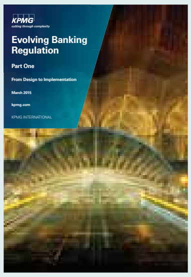
National implementation of international standards 16

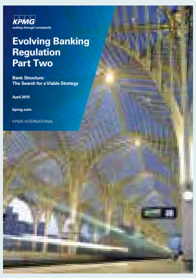
Annex 1: International standards 20

Annex 2: Examples of national regulation and supervision relating to corporate governance 22

Abbreviations 27

Evolving Banking Regulation – Parts One, Two and Three





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

The final part of *Evolving Banking Regulation* will focus on **conduct and culture.**

Executive summary

> An effective board is one which understands the business, establishes a clear strategy, articulates a clear risk appetite to support that strategy, oversees an effective risk control framework, and collectively has the skills, the experience and the confidence to hold executive management rigorously to account for delivering that strategy and managing within that risk appetite.
>
> **UK Prudential Regulation Authority,** May 2015

Analysis of the financial crisis revealed poor quality decision-making and poor quality oversight of risk by many bank Boards. The governance of many banks was at best fractured, and at worst broken.

Banks face commercial, shareholder and regulatory pressures to improve their governance.

Most banks recognise the **commercial advantages of good governance** – not least to improve both strategic and day-to-day decision-making and risk management; to support senior management in executing their responsibilities; and in particular to support the implementation of an unprecedented level of strategic change in response to competition, technology, data, structure and regulation.

Meanwhile, **standard setters have begun to define what good governance looks like**, with a particular focus on the role of the Board[1] and on risk governance. This paper therefore concentrates on these aspects of corporate governance.

Banks then face the challenge that even when they have met the expectations of their regulators and supervisors they also need to meet the commercial imperative to deliver real benefits from this.

International standard-setters and national authorities have strengthened their rules and guidance on governance; and **supervisors** have increased the intensity and widened the scope of their interactions with banks' Boards and senior management.

The focus of this enhanced regulation began with **remuneration**, reflecting the initial post-financial focus of the G20 and national politicians.

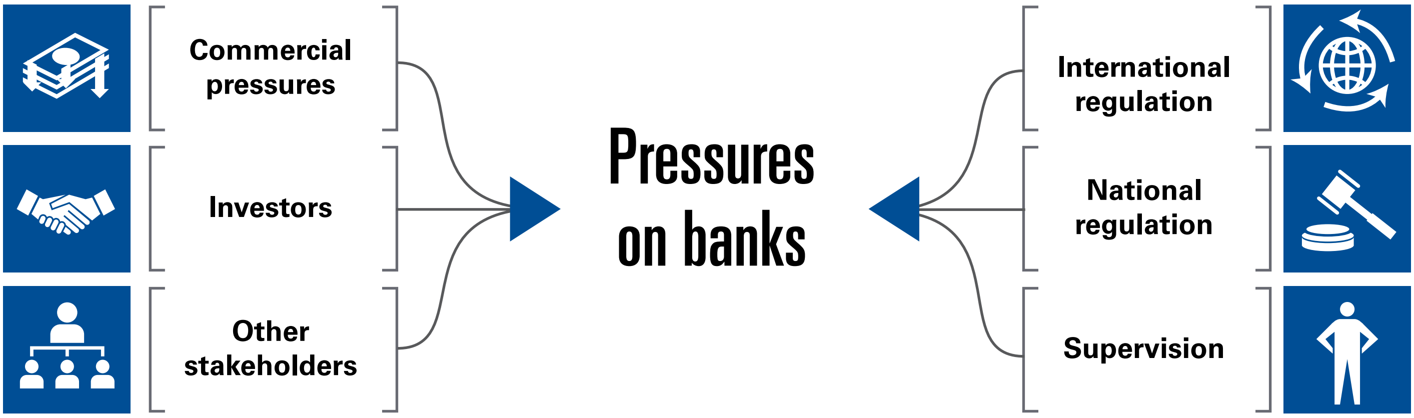
Regulatory and supervisory attention was then extended to **improving the functioning of some long-standing areas of governance** where banks had less focus ahead of the financial crisis. These include the **separation of the roles** of the Chair of the Board and the CEO; the **knowledge, experience, expertise, independence and time commitment** of the non-executive directors, and the extent of the **challenge** they provide; and various specific aspects of **risk governance**.

Most recently, the focus has widened to the role of Boards in establishing, communicating and assessing the **culture, value and behaviours** of the bank; the **assessment** (by banks and their supervisors) **of the suitability** of Board members and senior management; and **holding senior management personally accountable** for their bank meeting regulatory requirements and expectations.

The **regulatory consequences of poor governance in banks have become clearer**. Supervisors have become increasingly active and tougher in directing banks to improve their governance; in assessing the suitability of new senior managers and Board members; in making more use of Pillar 2 capital add-ons in response to poor governance and controls; and in taking disciplinary action – against banks and where possible against individuals – when serious problems emerge. There is less solid evidence of investor pressure being brought to bear on banks.

Banks have improved their governance, in part in response to these commercial, regulatory and supervisory pressures. At Board level, we observe more attention being focused on understanding risk, on setting risk appetite, and on controlling, measuring, monitoring and reporting risk. This includes a reinforcement of the Board with non-executive directors who bring a deeper experience and expertise of banking and risk management; a more active role for the Board Risk Committee;

[1] "Board" refers here to either a unitary Board, or the Supervisory Board in a dual board structure.



a closer consideration of risk maps and risk related management information; and establishing and elevating the role of the CRO in discussing risk with the Board Risk Committee and/or the Board itself.

However, **further progress** in some key areas of governance is needed:

- Clarifying who owns corporate governance issues in a bank;
- Demonstrating that an effective risk governance framework is in place and is operating as intended, and that the bank is capable of being governed effectively;
- Finding sufficient qualified, experienced and fully independent Board members, especially in countries with smaller talent pools;
- Reaching a sufficiently advanced Board level understanding of risk;
- Defining a risk appetite for difficult to quantify risks, setting risk limits across business units and entities, strategic planning and execution, and embedding risk appetite within a wider risk culture;
- Ensuring that desired culture and values are not only stated but are firmly embedded throughout the bank and reinforced through recruitment, remuneration and promotion decisions;
- Establishing clear personal responsibilities for the senior management team, individually and collectively, and enforcing accountability for these responsibilities;
- Introducing data aggregation and reporting procedures that are capable of supporting accurate regulatory reporting, good risk management and effective Board oversight (as discussed in Part Three of *Evolving Banking Regulation*);
- Making the CRO role fully effective in reaching a full group-wide, forward-looking and strategic view of risk, and using this to add value to both Board oversight and the risk management function; and
- Identifying and controlling conduct risk (in both retail and wholesale markets).

To make further progress, banks may find it useful to:

- **Undertake a self assessment against regulatory core standards and principles,** together with the expectations of other stakeholders.
- **Clarify how improved governance will be measured from a commercial perspective;** and
- **Seek independent assurance of progress made and the gaps still to be addressed**, from some combination of internal audit, third party reviews and Board effectiveness reviews.

Key issues for banks

Governance issues	Gaps banks need to address
Board composition: • Independence • Expertise (individual and collective) • Understanding • Time commitment • Chair/CEO separation	🟢 Mostly addressed by banks 🟡 Finding sufficient qualified, experienced and fully independent Board members, especially in smaller countries
Board (and Board committees) roles: Strategy, culture and values Risk appetite statement driving limits and controls Identification of high level risks and related controls Independent view of risk Gaining assurance that controls operate effectively Oversight of implementation of effective risk management systems Stress testing, ICAAP and ILAAP Succession planning, BCP and recovery and resolution planning	🟢 Banks making progress in these areas, but still some areas for improvement 🔴 Communicating and embedding culture and values 🟡 Defining a risk appetite for difficult to quantify risks 🟡 Identifying and controlling conduct risk
Control functions: Risk management, compliance, finance, internal audit • Independence, resourcing, authority and scope • IT infrastructure • Data aggregation • CRO independence, reporting lines, and access to the Board	🟡 Introducing fully effective data aggregation and reporting procedures 🟡 Enhancing the effectiveness of the 'three lines of defence' 🟡 Making the CRO role fully effective in reaching a full group-wide, forward-looking and strategic view of risk
Clarity of responsibilities and personal accountability	🔴 Establishing clear personal responsibilities for senior management and enforcing accountability for these responsibilities
Remuneration	🟢 Banks have generally adapted to post-financial crisis constraints on variable remuneration
Independent assessment of • Board effectiveness • Risk governance framework • Control functions	🟡 Banks still have progress to make on assessing and demonstrating independently the quality of their governance and controls

Key:
🔴 significant gaps remaining
🟡 some gaps remaining
🟢 mostly dealt with

National regulation and supervision	International standards
Reasonably consistent national measures, especially in Europe where based on CRD4	BCBS Principles CRD4 EBA SREP Guidelines
High level consistency driven by use of FSB and BCBS standards as a starting point But considerable variation in the detail of national standards Also differences in national supervisory approaches, but with some common themes in terms of moving towards: • On-site reviews of risk governance • Meetings with Board members and senior management • Attending Board meetings • Enhanced reporting requirements on Board and sub-committee minutes, risk management practices, stress testing Differences in supervisory responses to governance failings in banks – requests for improvement, use of Pillar 2 capital add-ons, enforcement actions Supervisory difficulties in assessing culture	FSB on risk governance, risk appetite and risk culture BCBS Principles EBA SREP Guidelines
National measures mostly high level, leaving the detail open to interpretation open to banks and their supervisors Considerable supervisory attention on data aggregation and reporting, in particular for larger and more complex banks	BCBS Principles FSB on risk governance BCBS on data aggregation and reporting EBA SREP Guidelines
Even within the EU, divergences in supervisory assessments of 'fit and proper' UK Senior Managers Regime	EBA Guidelines IOSCO
Reasonably consistent national measures, based on FSB Principles (supplemented in Europe by CRD4)	FSB Principles and Implementation Standards BCBS Principles CRD4 EBA SREP Guidelines
Some national measures to require banks to self-assess, but use of this by supervisors less clear	BCBS Principles

Banks: Further progress needed

Banks are telling KPMG across the EMA region that supervisory pressure on them in the area of corporate governance is increasing. Some large banks in the euro area, now supervised by the ECB, report being surprised by the ECB's 'deep dive' into governance, including the more intrusive techniques (on-site attendance at executive committee meetings, and interviews with key function holders) and questioning (for example, of why Boards believe that their risk appetite framework is appropriate and that the information reported by management to the Board is accurate and appropriate).

This supervisory pressure takes various forms across jurisdictions, with the most frequent being supervisory inspections, meetings with Board members, requests for documentation, self-certification that a bank meets local requirements, more intensive supervisory assessment of new director appointments and closer scrutiny of the independence of non-executive directors, and requests for Boards to undertake effectiveness reviews.

In response, banks report a wide range of initiatives to improve their corporate governance and their ability to respond to supervisory challenges.

Areas of improvements on which EMA banks are focusing include:

Current areas of focus

A greater focus on risk at Board level

- Greater Board involvement in risk management;
- Establishing and embedding a risk culture;
- Establishing a risk appetite framework;
- Establishing a Board Risk Committee, and the respective roles of Audit and Risk Committees;
- Appointing more experienced non-executive directors; and
- Training of non-executive directors on governance and regulatory matters.

Reinforcing the three lines of defence

- Embedding more risk management in the first line of defence (the business units), shifting the business units from being almost entirely revenue-driven to being more risk-constrained and obligation-driven;

- Making the second line (including risk management) more dominant, more powerful, and more centralised; and
- Enhancing the third line (including internal audit) to provide more robust assurance that systems and controls are operating effectively.

Enhancing the risk management function

- Increasing the independence and resources of the risk management function; and
- Appointing a CRO – many banks have reviewed and revised the role, responsibilities and reporting lines of the CRO, and in doing so have generally enhanced the CRO function. In line with the FSB guidelines, CROs increasingly report directly to the CEO rather than through the Chief Financial Officer (CFO), and have much greater access to the Board and the Board Risk Committee.

Introducing risk-related remuneration

- As observed in the FSB's latest (November 2014) update on compensation practices, most banks have attained a high level of implementation of the 2009 FSB Sound Compensation Practices;
- However, the FSB also notes that supervisory findings indicate a number of areas for improvement by banks, including governance, identification of material risk takers, risk alignment and ex post adjustments (malus and clawback);
- In the EU, some further changes in compensation structures are necessary to meet CRD4 requirements, in particular for the remuneration of material risk takers in a bank;
- Improving governance frameworks for compensation, including the role of the Board and Board Remuneration Committee in considering the incentive structures for risk-taking and customer-facing staff at all levels of a bank; and
- Establishing risk-adjustment metrics across all relevant products and services.

Data and IT governance

- As discussed in Part Three of *Evolving Banking Regulation*, banks are seeking to improve the quality of their data and their IT systems for the purposes of risk management and risk reporting, including for reporting to the Board and Board Risk Committee.

Some banks are also preparing additional documentation to explain their governance approach to their supervisors; establishing dedicated corporate governance units under the Board Secretary or Compliance Department to handle corporate governance matters and ensure full compliance with regulatory requirements; and seeking to link their own self-evaluations with supervisory timelines and area of interest.

Need for further progress

Some banks and some countries have made more progress than others in these areas of improvement, but many banks continue to report that they need to make further progress in:

Board composition

- Finding sufficient **qualified, experienced and fully independent Board members**, especially in smaller countries;

Board roles

- **Enhancing their risk culture**, to include embedding a clear set of values and culture at all levels of the organisation, learning from risk culture failings, and encouraging internal challenge to perceived poor behaviours;

- **Implementing and documenting Board oversight** to demonstrate the effectiveness of the Board's monitoring role and the follow-up of the actions taken;

- **Defining a risk appetite** for difficult to quantify risks, setting risk limits across business units and entities, and embedding risk appetite within a wider risk culture;
- Balancing centralised group risk management, decision making and control with the need to demonstrate that the **local Board of each regulated entity remains accountable for the viability, sustainability and resolvability of that entity**;

Control functions

- **Meeting all regulatory requirements and supervisory expectations**, and keeping up with the changing regulatory environment;
- Meeting regulatory requirements for the **independence of risk management**, especially in smaller banks;
- Enabling a CRO to establish a **genuinely group-wide view of risk**, in particular with respect to the capital, funding and liquidity issues that have traditionally been the responsibility of the CFO; and to business activities or geographies that have traditionally been managed independently;
- Enhancing the **capability of the CRO and the risk management function** more generally to take a forward-looking and strategic view of risk, not just a reactive and backward-looking monitoring of limits and procedures;
- Further **investment and up-skilling in all three lines of defence** – the first line to enable it to focus more effectively on risk management, the second line to focus on advice, framework design, effective challenge and risk aggregation to identify concentrations and correlations across the bank, and the third line to provide positive assurance on the effectiveness of risk policies, processes and controls;
- **Recruiting sufficient experienced and qualified staff into control functions**, due to budgetary constraints and the lack of available experience;
- **Improving data quality, IT systems and risk reporting** – at many banks the shift from pre-crisis inadequacy and fragmented oversight to much improved group-wide risk data aggregation and reporting to the Board on a timely basis remains incomplete;

Clarity of responsibilities

- **Defining roles and responsibilities** for new risk management and risk reporting procedures;

Remuneration

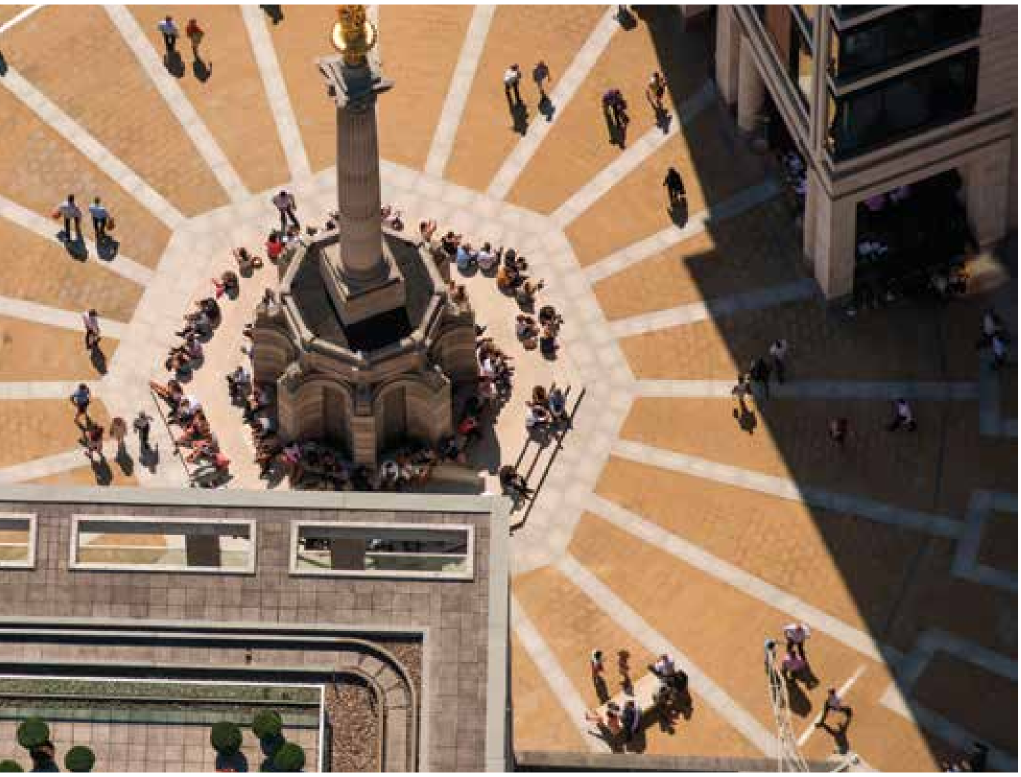
- Implementing a **remuneration framework** that genuinely reflects performance against compliance and risk management;

Board effectiveness

- **Showing how good risk management adds value** within the bank;
- Some banks mention that **recent regulatory trends have shifted the focus of bank Boards too much towards compliance**, at the expense of discussions of strategy and business performance; that supervisors are prescribing governance structures that are not driven by the bank itself; and that a 'one size fits all' regulatory approach is damaging to small, domestic and private banks.

To make further progress, banks should:

- **Consider how meeting regulatory and supervisory expectations can be converted into a commercial advantage;**
- **Consider how governance issues can best be brought to life, by focussing on the substance and the desired outcomes rather than solely on the form and the necessary inputs;**
- **Undertake a self assessment against regulatory core standards and principles, together with the expectations of other stakeholders.** One key question for banks here is how they can demonstrate that they are meeting (or where necessary are taking action to enable them to meet) regulatory requirements and other expectations, and in doing so are delivering the real substance and spirit of good governance, not just the form and the letter; and
- **Seek independent assurance of progress made and the gaps still to be addressed**, from some combination of internal audit, third party reviews and Board effectiveness reviews.



International standard-setting

There have been few recent international standard-setting initiatives on governance-related topics, perhaps reflecting the lack of anything new to say on standards.

Both the main initiatives relevant to banks – from the Basel Committee and the European Banking Authority (EBA) – have largely brought together existing material in order to provide updated compendiums of material on governance.

Meanwhile, earlier published standards from the Financial Stability Board (FSB) and the EU Capital Requirements Directive (CRD4) continue to be transposed into national legislation, rules and guidance and to be implemented by banks.

It would be difficult to argue with any of these statements. There is little new left to say about good governance. The challenge here for banks is to bring this alive in a way that also delivers commercial advantage.

Basel Committee Corporate Governance Principles

The Basel Committee updated its corporate governance principles in July 2015 (see Annex 1), replacing the previous version that dated back to 2010.

The main changes since the previous version seek to reinforce the collective oversight and risk governance responsibilities of the Board by:

- Expanding the guidance on the role of the Board in **overseeing the implementation of effective risk management systems;**
- Emphasising the importance of the **collective competence of the Board**, as well as the obligation of individual Board members to dedicate sufficient time to their mandates and to keep abreast of developments in banking;
- Strengthening the guidance on **risk governance**, including the specific risk management roles and responsibilities of the Board, Board risk committees, senior management, business units and the control functions, including the CRO and internal audit;
- Underlining the importance of the Board setting the "tone at the top" and overseeing management's role in fostering and maintaining a **sound corporate and risk culture**;
- Recognising the importance of **compensation systems** in conveying acceptable risk-taking behaviour and reinforcing risk culture; and

- Emphasising the responsibility of the Board and senior management to define and manage the **conduct risk** inherent in a bank's business.

EBA SREP Guidelines on Corporate Governance

Although the EBA's SREP Guidelines (December 2014) are directed primarily at banking supervisors, they also provide a clear statement of the standards that banks should be able to demonstrate.

Supervisors are expected to include in their risk assessment of a bank:

Organisation and functioning of the Board – adequate number and composition of members, who are fit and proper and demonstrate a sufficient level of commitment and independence; the effectiveness of the Board is reviewed; appropriate internal governance practices and procedures.

Overall governance framework – the Board knows and understands the operational structure of the bank and the associated risks.

Corporate and risk culture – the Board sets the bank's strategy and corporate values. The bank's corporate and risk culture is communicated effectively, creates an environment of challenge in which decision-making processes promote a range of views, and is applied across all levels of the bank.

Risk management framework – considers all material risks to which the bank is exposed and contains risk limits consistent with the bank's risk appetite; forward-looking, in line with the strategic planning horizon, and regularly reviewed; stress testing embedded, with Board and senior management involved, and integrated into decision-making.

Internal control framework – first line (business units) of defence responsible in the first instance for establishing and maintaining adequate internal controls; independent second (risk and compliance) and third (internal audit) lines of defence; clear allocation of responsibilities; policies and procedures to identify, measure, monitor, mitigate and report risk; risk control function actively involved in drawing up the bank's risk strategy, in all material risk management decisions, and in providing the Board and senior management with all relevant risk-related information; CRO with a sufficient mandate and independence.

Information systems – generate accurate and reliable risk data in a timely manner; capture and aggregate all material risk data across the bank; support risk data capabilities at normal times as well as during times of stress.

Remuneration – remuneration policy maintained, approved and overseen by the Board, in line with the bank's values, business strategy, risk appetite and risk profile; does not incentivise excessive risk-taking; appropriate combination of variable and fixed remuneration.

FSB standards on risk governance

The Financial Stability Board (FSB) published in February 2013 a set of **sound risk governance practices**, based on national regulatory and supervisory developments since the financial crisis, and on a review of risk governance practices in 36 major banking groups across the G20 area.

The sound risk governance practices (see Annex 1) emphasise the critical role of the Board and the Board risk committees in strengthening a bank's risk governance, through their involvement in promoting and evaluating a strong risk culture in the organisation; establishing and communicating the bank's risk appetite; and overseeing management's implementation of the risk appetite and overall risk governance framework.

The FSB extended its guidelines on risk governance with two further papers: a set of Principles for an **effective risk appetite framework** (November 2013 – see Annex 1), and Guidance to supervisors on **assessing the risk culture of financial institutions** (April 2014).

The FSB's Guidance on **assessing risk culture** is intended to help supervisors to understand a bank's risk culture, in particular whether it supports appropriate behaviours and judgements within a strong risk governance framework.

The FSB recommends that supervisory interaction with Boards should be stepped up, based on high-level sceptical conversations with the Board and senior management on the bank's risk appetite framework; and on whether the bank's risk culture supports adherence to the agreed risk appetite and to sound risk management.

Supervisors will be expected to focus on four key 'risk culture indicators':

1. **Tone from the top** – how the bank's leadership ensures that its core values are communicated, understood, embraced and monitored throughout the organisation. This includes leading by example, assessing the impact of the high level values on behaviour throughout the bank, ensuring common understandings of risk, and learning from risk culture failures.
2. **Accountability** – a clear allocation of risk ownership, escalation processes, and internal enforcement procedures.
3. **Effective challenge** – encouraging challenge and dissent, and organising the risk functions to provide access of risk and compliance to senior management and the Board.
4. **Incentives** – basing remuneration on adherence to risk appetite and to desired cultures and behaviours, and appropriate talent development and succession planning.

CRD4 standards on corporate governance

CRD4 contains a set of **corporate governance requirements**, which focus primarily on:

Roles and responsibilities of the Board and its committees – The Board should approve and oversee strategy, risk strategy and internal governance, and there should be independent risk and remuneration committees, entirely composed of non-executive directors.

Board composition – limitations on the number of directorships which may be held by members of the Board at any one time; a separation of the roles of Chairman and CEO; and appropriate Board skills, diversity of experience, honesty and integrity.

Remuneration – Banks should set a remuneration policy which is consistent with sound and effective risk management and business strategy. Individuals in compliance and risk management should be remunerated appropriately and independent of the performance of the business they control. Variable remuneration should be assessed on a multi-year framework, guaranteed variable remuneration should be avoided except in exceptional circumstances, and variable remuneration should not be more than 100 percent of base salary.

Remuneration

The FSB's third (November 2014) progress report on the implementation of the FSB Principles for Sound Compensation Practices (April 2009) and their Implementation Standards (September 2009) concluded that implementation of these principles and standards has been essentially completed, although several jurisdictions continue to refine their regulatory framework or guidance on compensation practices.

National implementation of international standards

Although national laws, regulation and guidelines have broadly followed the international standards discussed above, this has not resulted in a fully consistent calibration and implementation across jurisdictions. This is evident in both the development of national standards and the application of these requirements and expectations by national supervisors. It is not clear to what extent monitoring through country and peer reviews by the FSB and the Basel Committee (and, within the EU, by the EBA) will deliver greater consistency here.

This paper is informed by contributions from KPMG experts in countries from across the EMA region on developments in national regulation and supervision, and on the responses of banks to these developments.

Regulation

New national rules and guidance (see Annex 2) have typically included requirements on banks to:

- Undertake more detailed Board oversight of risk and risk management;
- Strengthen the composition of the Board and its sub-committees, including the independence, expertise, time commitment and diversity of non-executive directors;
- Clarify individual responsibilities and accountability;
- Establish a Board Risk Committee;
- Enhance the risk management function and the role of the Chief Risk Officer (CRO), in terms of independence, expertise, stature, authority and scope;
- Introduce risk-adjusted variable remuneration, with scope for claw-back; and
- Undertake independent assessments of the bank's risk governance framework, through Board effectiveness reviews, internal audit assurance reviews and third party assessments.

In the EU, some of these areas have been covered though the transposition of CRD4 into national requirements.

Meanwhile, some national initiatives may gain traction elsewhere, in particular the Senior Managers Regime and the outcome of the Fair and Effective Markets Review in the UK.

Regulators and supervisors outside the UK are following these developments with interest, so there is likely to be some read-across to banks in other countries.

UK Senior Managers Regime

The new UK **Senior Managers Regime** (SMR) – which is due to come into effect from March 2016 – was developed in response to political concerns that the Approved Persons 'fit and proper' regime had failed to prevent some unfit individuals from taking up senior positions in banks, and had been ineffective in providing a basis for taking disciplinary action against the senior management of banks that needed public support during the financial crisis.

The main objective of the SMR is to enhance the accountability of senior management for meeting their responsibilities.

Key issues for banks in implementing the SMR include:

- Building a governance model around the SMR;
- Identifying 'senior managers' and clarifying their individual responsibilities and the overall responsibilities map;
- Clarifying the governance framework (group Board and committees, legal entity level Board and committees, executive management committees), to ensure that it is consistent with the set of individual senior manager responsibilities;
- Introducing policies and procedures to operate the Senior Manager and Certification Regimes;
- Aligning the new regimes with the broader transformation in culture and banking standards; and
- Meeting evidential requirements to demonstrate that senior managers have taken reasonable steps to prevent regulatory breaches in their areas of responsibility, and that the bank is properly supervising and certifying staff under the Certification Regime.

The **key new elements of the SMR** are that:

- It will apply to a narrower range of individuals than the Approved Persons regime, being limited to the most senior executives responsible for those areas of a firm which the PRA deems relevant to its safety and soundness objective, such as its overall business, financial resources, risk management, internal controls and key business areas, and to the key oversight functions of the Chair of the Board, Chairs of Board committees, and the senior independent director;
- Banks will be required to specify the individual responsibilities of these 'senior managers' (including responsibilities prescribed by the PRA or FCA), and to establish a mapping of senior management responsibilities to demonstrate how the set of responsibilities fits together;
- An earlier proposal to subject senior managers to a 'presumption of responsibility' for regulatory breaches has been replaced by a statutory duty on senior managers to take reasonable steps to prevent regulatory breaches in their areas of responsibility; and
- Senior managers will potentially be subject to criminal sanctions for reckless mismanagement of a bank.

The SMR is supplemented by a **Certification Regime**, which applies to remaining significant influence functions, material risk takers (as defined in CRD4), and customer-facing staff of banks, under which these staff must be supervised by the bank and be certified annually by the bank as fit and proper. These staff are potentially subject to civil sanctions.

In addition, all non-ancillary staff (including non-executive directors) will be subject to **Conduct Rules**. These rules will require all these staff to act with integrity, due skill, care and diligence, and be open and transparent with regulators; and will require senior managers to take reasonable steps to ensure that the business of the bank for which they are responsible is controlled effectively, and complies with the relevant requirements and standards of the regulatory system, and that any delegation of their responsibilities is to an appropriate person and that they oversee effectively the discharge of the delegated responsibility.

UK Fair and Effective Markets Review

The UK authorities published the final report of the Fair and Effective Markets Review in June 2015. The Review was established a year earlier, following a number of high profile abuses in the wholesale Fixed Income, Currency and Commodity (FICC) markets. Although a review rather than a legislative proposal, market participants should not be complacent about the potential scale of change likely to come to the FICC markets both in the UK and elsewhere.

The Review identifies a need for further progress in a number of areas that relate to governance:

Holding individuals to account for their own conduct

- Extending UK criminal sanctions for market abuse to a wider range of FICC instruments;
- Lengthening the maximum sentence from 7 to 10 years' imprisonment;
- Extending elements of the Senior Manager and Certification Regimes to a wider range of regulated firms active in FICC markets; and
- Mandating qualification standards to improve professionalism.

Taking coordinated international action to improve fairness and effectiveness

- Encouraging IOSCO to consider developing a set of common standards for trading practices that will apply across all FICC markets. IOSCO announced in June 2015 that it will work to strengthen further the current global framework to address misconduct by firms and individuals in retail and wholesale markets. This global review of conduct standards is likely be closely aligned with the international issues identified by the UK's Fair and Effective Markets Review;
- Agreeing a single global FX code providing a comprehensive set of principles to govern trading practices around market integrity, information handling, treatment of counterparties and standards for venues. A BIS working group on strengthening code of conduct standards and principles in foreign exchange markets commenced work in July 2015; and
- Examining ways to improve the alignment between remuneration and conduct risk at a global level.

Key issues for banks include:

- The potential overlaps between the banking and FICC Senior Manager and Certification Regimes;
- The introduction of further detailed measures specific to FICC markets may cut across the wider-ranging need to improve culture and behaviours across all of a bank's activities; and
- The end result of the global outreach – as we have seen with other international principles, differences in the detail can lead to operational challenges for the banks affected and potentially open up opportunities for regulatory arbitrage.

Supervision

Together with the introduction of new and revised international and national standards, supervisors have **increased the intensity and intrusiveness** of their assessment of banks' corporate governance. Supervisory expectations have increased in key areas such as risk governance, risk appetite frameworks and risk culture.

This has taken various forms (see Annex 2), including:

- Supervisors taking a **more active and intensive approach to fit and proper assessments** of candidates for Board and senior management positions, and in some countries the scope of such assessments has been broadened to include all relevant staff that can materially influence a bank's risk position (see box on page 19);
- **On-site reviews** of risk governance, including risk appetite frameworks;
- Supervisors **attending Board meetings**;
- **Enhanced dialogue** with banks at Board and senior management levels, including meetings with non-executive directors and more substantive discussions on risk governance, culture and risk appetite;
- **Enhanced reporting requirements** on banks' risk management practices, including information on exposure limits, stress testing, Board and sub-committee minutes, and reports on risk governance from external auditors and other third parties. In some cases, greater supervisory intensity has resulted in a considerable increase in the number, frequency, and scope of data requests from supervisors to banks; and
- **Supervisory actions when governance failings are identified**, through requests to banks to improve their governance, higher Pillar 2 capital add-ons, and in some cases enforcement actions.

However, **supervisory assessments of culture** remain at an early stage of development for most supervisory authorities. Supervisors are uncertain about how to review and assess a bank's culture – not least how to determine the extent of buy-in at all levels of the bank – and how to integrate this into the overall risk assessment of the bank.

Meanwhile, the FSB's progress report (November 2014) on **compensation practices** noted that the assessment of compensation practices has become an essential part of the supervisory cycle for many national authorities. There are, however, important differences across jurisdictions in:

- Some areas of scope, such as the identification and treatment of material risk takers in banks;
- The extent of variable pay that is required; subject to deferral; and 'at risk' under a malus or clawback mechanism;
- The frequency and intensity of the supervision of banks' compensation practices (including in the use of on-site inspections, horizontal reviews and continuing dialogue with banks); and
- Supervisory actions in response to findings on banks' compensation practices.

The FSB's thematic review on supervisory frameworks and approaches for SIBs (May 2015) also highlighted some key outstanding challenges on **supervisory effectiveness**. Those relevant to corporate governance include:

- The need to establish and implement clear and transparent supervisory strategies and priorities against which supervisory effectiveness can be more objectively assessed;
- Maintaining high-level, constructive dialogue with institutions at a senior level to support supervisory judgement and risk assessment;
- Ensuring that requests for data and other information genuinely support a more detailed and informed approach to supervisory understanding of banks' key strategic choices and related risks and vulnerabilities;
- For international banks, reaching a common understanding and assessment of key risks and supervisory priorities across jurisdictions; and
- Building and maintaining a skilled, capable, and experienced supervisory workforce.

ECB thematic review of governance

The ECB has conducted a thematic review of governance and risk appetite in the 123 major banks supervised directly by the ECB, based on the governance element of the EBA's SREP Guidance. This in turn has fed into the ECB's risk assessments of these banks, and into the Pillar 2 capital requirements for these banks.

The ECB's findings indicate that even where banks may meet existing national requirements they do not always comply with the emerging international good practice standards with regard to governance.

Particular issues identified by the ECB include:

Board composition – a lack of relevant knowledge and expertise among non-executive Board members; concentrations of power in individual Board members; information asymmetries among Board members; a lack of independence of non-executives who have been on a Board for many years; in some cases a concern that some non-executives may be subject to political influence; and an identified need for a more clearly defined role for a senior independent non-executive director who can channel the concerns of the non-executive directors.

Board role – some Boards do not take enough time to discuss and reflect on individual issues; the risk appetite framework is not always properly formulated and applied consistently throughout the entire bank; and some Boards do not focus sufficiently on succession planning for senior management positions.

Control functions – a lack of separation between a bank's risk and audit functions.

Fit and proper regimes across the EU

The EBA's peer review (June 2015) of the national implementation of EBA Guidelines on the assessment of the suitability of Board members and other key function holders showed significant divergences in regulatory and supervisory practices, even though most countries met the high level Guidelines.

The main differences included:

- **Scope** – differences across countries in which key function holders are subject to a fit and proper regime;
- **Definition of suitability** – differences in requirements on banks' own assessments of suitability; the information required by national authorities; time frames for reaching decisions; and mandatory periodic re-assessments of suitability;
- **Criteria used to assess suitability** – differences in the criteria used to indicate (lack of) good reputation and to assess experience; the intensity of screening; the level of documentation; and the use of interviews;
- **Collective (Board-wide) assessment of 'fit and proper'** – differences in the use of 'face-to-face' meetings with members of the Board; and attending Board meetings;
- **Independence and conflict of interest** – differing views on how these are interpreted;
- **Supervisory intensity** – differences in the assessment of governance within the supervisory review and evaluation process; and the use of specialist expertise.

In response, the EBA is proposing to:

- Clarify the scope of a fit and proper regime;
- Extend its existing definitions and criteria to include individual knowledge, skills, integrity, independence, time commitment and potential conflicts of interest, and collective knowledge and experience;
- Develop a template for fit and proper assessments for banks to use and to submit to national authorities;
- Promote the use of interviews for certain categories of applicant;
- Promote enhanced cooperation among national authorities where candidates have previously worked in another country; and
- Encourage national authorities to consider the use of pre-approval for Board positions; exit interviews; attending Board meetings and one-to-one meetings with Board members; and requesting detailed minutes of Board meetings.

Annex 1: International standards

Basel Committee Corporate Governance Principles (July 2015)

Principle 1: Board's overall responsibilities

The Board has overall responsibility for the bank, including approving and overseeing management's implementation of the bank's strategic objectives, governance framework and corporate culture.

Principle 2: Board qualifications and composition

Board members should be and remain qualified, individually and collectively, for their positions. They should understand their oversight and corporate governance role and be able to exercise sound, objective judgment about the affairs of the bank.

Principle 3: Board's own structure and practices

The Board should define appropriate governance structures and practices for its own work, and put in place the means for such practices to be followed and periodically reviewed for ongoing effectiveness.

Principle 4: Senior management

Under the direction and oversight of the Board, senior management should carry out and manage the bank's activities in a manner consistent with the business strategy, risk appetite, remuneration and other policies approved by the Board.

Principle 5: Governance of group structures

In a group structure, the Board of the parent company has the overall responsibility for the group and for ensuring the establishment and operation of a clear governance framework appropriate to the structure, business and risks of the group and its entities. The Board and senior management should know and understand the bank group's organisational structure and the risks that it poses.

Principle 6: Risk management function

Banks should have an effective independent risk management function, under the direction of a chief risk officer (CRO), with sufficient stature, independence, resources and access to the Board.

Principle 7: Risk identification, monitoring and controlling

Risks should be identified, monitored and controlled on an ongoing bank-wide and individual entity basis. The sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, to the external risk landscape and in industry practice.

Principle 8: Risk communication

An effective risk governance framework requires robust communication within the bank about risk, both across the organisation and through reporting to the Board and senior management.

Principle 9: Compliance

The bank's Board of directors is responsible for overseeing the management of the bank's compliance risk. The Board should establish a compliance function and approve the bank's policies and processes for identifying, assessing, monitoring and reporting and advising on compliance risk.

Principle 10: Internal audit

The internal audit function should provide independent assurance to the Board and should support Board and senior management in promoting an effective governance process and the long-term soundness of the bank.

Principle 11: Compensation

The bank's remuneration structure should support sound corporate governance and risk management.

FSB sound risk governance practices (February 2013)

- Independence and expertise of the Board;
- Role of the Board in establishing and embedding an appropriate risk culture throughout the firm;
- Membership and terms of reference of the risk and audit committees;
- Independence, role and reporting lines of the CRO (direct to the CEO, not through the CFO);
- Importance of CRO involvement in all significant group-wide risks (including treasury and funding) and in key decision-making processes (including strategic planning, acquisitions and mergers);
- Independence, authority and scope of the risk management function; and
- Independent assessment of the risk governance framework.

FSB Principles for an effective risk appetite framework (November 2013)

An effective risk appetite framework should act as a brake against excessive risk-taking, and should be:

- Driven by both the Board and management at all levels;
- Communicated, embedded and understood across the bank;
- Used as a tool to promote robust discussions of risk and as a basis upon which the Board, risk management and internal audit functions can challenge management recommendations and decisions; and
- Adaptable to changing business and market conditions.

This requires:

A **risk appetite statement** that:

- Is linked to the bank's short- and long-term strategic, capital and financial plans;
- Establishes for each material risk the maximum amount of risk the bank is prepared to accept;
- Includes quantitative measures that can be translated into risk limits applicable to business lines, legal entities and groups; and
- Is forward looking and subject to scenario and stress testing to ensure that the bank understands what events might push the bank outside its risk appetite and/or risk capacity.

Risk limits that:

- Constrain risk-taking within risk appetite;
- Are established bank-wide and for business lines and legal entities;
- Do not simply default to regulatory limits, and are not overly complicated, ambiguous, or subjective; and
- Are monitored regularly.

A set of supporting **roles and responsibilities** – the Principles include detailed job descriptions that outline the roles and responsibilities of the Board, CEO, CRO, CFO, business heads and internal audit with respect to the risk appetite framework.

Annex 2: Examples of national regulation and supervision relating to corporate governance

Country	National regulation	National supervisory focus	Supervisory actions in event of governance failings
ECB	The ECB assesses governance on the basis of FSB and Basel Committee Principles and other standards, the EBA SREP Guidelines, and national transpositions of CRD4	Thematic review of corporate governance, focused mainly on risk governance and risk appetite Assessment against relevant parts of EBA SREP Guidelines Documentation review, supplemented by meetings with key function holders and on-site attendance at executive committee and other meetings Seeking greater harmonisation of national practices for 'fit and proper' assessments of new board members	Higher Pillar 2 requirements emerging on a consistent basis for ECB directly-supervised banks
Belgium	Implementation of CRD4 and some local initiatives	Questions from supervisors have led some banks to review Board and committee composition 'Fit and proper' policies made and implemented	Requests to banks to improve their practices and enforcement action, but not higher Pillar 2 requirements so far
Finland	Implementation of CRD4	More intensive supervisory focus on corporate governance issues (especially risk management and internal control) in its supervision and when considering applications for authorisation Banks are more focused on board composition requirements	Supervisor has imposed administrative fines, public warnings and penalty payments
France	New rules in 2014 regarding the individual and collective capacity of Board members; the separation of executive (management) and non-executive (oversight) functions – a chairman of the Board can no longer also be the CEO; risk appetite; regulator has power to undertake audits on-site to check the risk culture of banks	Supervisory focus on the effectiveness of Board defined risk appetite statement, and the respect by business lines of the risk management function On-site analysis of the usefulness and consistency of risk dashboards sent by risk management function to Board and senior management	Limited to date

Germany	Minimum Requirements on Risk Management, including greater emphasis on risk concentrations (to address 'silo' problems in risk management); more detailed requirements for a risk control function; requirement to implement a compliance function; strengthening the interplay between management and the Board; and a requirement to have an appropriate compensation system and whistle-blowing process BaFin and the Bundesbank have articulated requirements regarding the responsibility and accountability of Board members	Supervisory focus on banks' risk management capacity All potential candidates for the Management Board at major banks are assessed by supervisors even if not required by law, and any dissatisfaction with the candidates is communicated to the bank Major banks asked to have proactive succession planning in place for Management Board positions Regular and ad hoc meetings and calls with Management Board Minutes of Board meetings checked on a regular basis Some Supervisory Board meetings of major banks are attended by supervisory staff	Employment of senior management cannot always be prohibited by law: moral suasion is necessary
Greece	Implementation of CRD4, with extended scope of regulatory requirements to new areas such as credit risk culture	During the last two years, the intensity of the supervision has increased, mainly in the area of non-performing loans risk management All systemic banks have updated the charters of the Board and other Committees, as well senior management job descriptions in order to comply with requirements In the context of the most recent recapitalisation of the four systemic Greek banks, the government announced the introduction of a periodic evaluation of banks' governing bodies and senior management against specific and objective criteria	Supervisors submit reports with recommendations. However, the follow up is not always prompt
Ireland	Local priorities and initiatives led to the statutory code requirements for credit institutions and insurance companies in 2011, and revised in 2013. The code covers • Minimum board size • Composition of the board • Independence of non-executive directors • Roles of the Chairman and CEO • Frequency of board meetings • Role and composition of a mandatory audit and risk committee	Governance is assessed as part of the ICAAP/SREP process	Instructions to banks to meet code requirements Higher Pillar 2 capital requirements

Italy	Wide range of regulatory requirements relating to risk governance, risk appetite and compensation, including: 2013 – Bank of Italy regulation on internal control systems, with a requirement on banks to define and implement a risk appetite framework (effective date July 2014) 2014 – Consob and Bank of Italy communication on policies and practice on remuneration (January); Bank of Italy communication regarding application of EBA guidelines on remuneration (October); Bank of Italy regulation on policies and procedures on remuneration (November) 2014 – Bank of Italy regulation on corporate governance (effective date from 2014 to 2017 depending on topic) – main changes relate to composition and functioning of the Board, with more prescriptive provisions on the competencies, composition and functioning of Boards 2015 – Governmental decree on 'popolari' banks (mutual banks) regarding corporate governance 2015 – Bank of Italy regulation in order to strengthen the internal control system with whistleblowing rules (effective end 2015)	Supervisors have always considered corporate governance topics during the last four years, for example during general supervisory inspections of banks; nevertheless, in 2014 the number of supervisory ad hoc inspections on corporate governance increased five-fold over 2013 Supervisory activity performed through an intense, extensive and challenging dialogue with banks, aimed at increasing Board engagement with the risk management framework and improving internal control systems Supervisory examination of Board effectiveness, taking into account both qualitative and quantitative factors Large-scale requests for objective and verifiable information Board self-assessment of internal skills, independence and integrity, individually and collectively	Requests to banks to improve practices are common, and supervisors requested higher Pillar 2 requirements from a number of banks during 2013 and 2014
Kuwait	Central Bank of Kuwait (CBK) instructions to all banks in Kuwait (issued in 2012 and effective from July 2013), based on FSB and Basel Committee principles, blended with local priorities. Include dedicated sections for risk management and internal controls, which provide detailed instructions related to risk governance within banks Banks required to develop criteria for board membership; the CBK has to approve all Board members and senior managers prior to their appointment. The Board as a whole and individual directors must be evaluated by the bank annually. CBK provides detailed instructions about non-Executive directors' roles and their positions on Board committees	Periodic inspections to assess the degree of implementation of required standards CBK stresses the independence of the CRO and direct reporting to the Board and Risk Committee	Disciplinary action, including fines

Latvia	CRD4 implementation	Supervisory focus for a number of years, covering most aspects of governance	Requests to improve governance, usually together with a fine
Malta	CRD4 implementation Requirement for a segregation between functions: even in small banks the CFO is not allowed to be responsible for risk At least two (previously one) non-executive directors at small banks	Additional due diligence carried out before approval of a director with a special focus on experience and proven expertise in the business of the bank. 'Fit and proper' requirements and enquiries have been intensified and reference letters have become an intrinsic part of the approval process	Banks are given a timeframe to address the deficiencies, following which the regulator will become more insistent, and will typically request a meeting with the Board
Netherlands	Implementation of CRD4	Regular discussions with Board members are part of the new supervisory approach Specialised staff (psychologists) have been hired to assist with the analysis of Board effectiveness More active use of 'fit and proper' assessments	Higher Pillar 2 capital requirements
Norway	Implementation of CRD4	More supervisory focus on governance in general, including in smaller banks	Request improvements
Qatar	Qatar Central Bank introduced corporate governance guidelines for banks operating in Qatar in 2012. Risk culture covered as part of these guidelines. Banks are required to report on their governance policies and procedures on an annual basis	More intensive monitoring of corporate governance practices, in particular in the area of Board independence and qualifications, Board composition and effectiveness, the role of non-executive directors, and risk culture Not yet been extended to senior management 'fit and proper' requirements	Relying on informal communication to improve practices Not yet taken steps to penalise banks for poor governance practices
Saudi Arabia	SAMA issued Internal Control guidelines based on the Basel Committee governance principles and the COSO framework, including a requirement for Internal Audit to verify and report on the internal control system to the Board on an annual basis Corporate Governance Regulation amended and updated by the Capital Market Authority – applicable on all the listed companies Collectively, the regulations cover the improvement of risk culture, the control environment, setting up a Board level Risk Committee, Board approval of risk appetite, Board risk policies, and the training of the Board	Greater supervisory focus on corporate governance Board members are asked to be involved in the approval of policies, setting the direction of the banks they govern, their individual training requirements and their monitoring and reporting On Board composition and effectiveness, supervisory emphasis on minimum number of Board meetings, independence of the Board, majority of non-executive directors, 'fit and proper' criteria for the selection of Board members and approval by the Central Bank	Mixture of actions, including following up actively with the banks to resolve issues highlighted in on-site inspections, and higher Pillar 2 requirements Enforcement actions can also be taken

South Africa	Implementation of FSB and Basel Committee standards, with some local adaptation New Board members and executives are required by regulation to apply to supervisory authority	Enhanced interaction with Boards and banks' management at various level of seniority Annual meeting with Board chair to discuss and assess effectiveness Board members are expected to provide a time matrix setting out their involvement on other Boards	Pillar 2 requirements and enforcement actions
Spain	Revised legislation and governance code to reflect both international standards and local initiatives New regulation in 2103 regarding fit and proper – increasing the assessment criteria and requiring internal procedures to be in place	Significant increase in supervisory focus on corporate governance, risk appetite, risk culture, compensation policies, compliance and risk management Review of the minutes of the Board, its committees and other internal bodies More meetings with senior management and at higher level. Plans to extend this to meetings with individual members of the Board	Requests to banks to improve practices and some enforcement actions
Sweden	Updated regulation in 2104 for governance and risk management, covering the organisational structure and the Board's understanding of it, corporate and risk culture, responsibilities of the Board, risk management, control functions and outsourcing requirements	Supervision has become more pro-active, interactive and transparent, and is characterised by intensive interaction with senior management of banks (more supervisory dialogue and moral suasion) Need to increase the frequency of interaction with the Board	
Switzerland	FINMA circular on Supervision and Internal Control (currently being revised to focus more on risk governance), and Stock Exchange guidelines on Corporate Governance for listed companies FINMA guidance on governance elements for the different areas of a bank, including remuneration of the Board and senior management	Periodic formal exchanges with Board and key committees (risk, compensation) More focus on the effectiveness of corporate governance Additional audits	Pillar 2 requirements and/or changes in the Board, enhancement of senior management
UK	Short and high level PRA supervisory statements on corporate governance, focusing on key elements of governance and controls – Board responsibilities (May 2015 consultation paper) and internal governance (updated August 2015) Senior Managers Regime to strengthen individual accountability at the most senior level in banks, shift the burden of proof when conduct or prudential failings arise at banks, and introduce a criminal offence of reckless conduct by senior bank staff Fair and Effective Markets Review	Deeper and more extensive interaction with major firms' Boards and senior management to enable better dialogue and challenge on those firms' risk management and decision making processes Assessment of major banks' governance arrangements Periodically observes Board and committee meetings Implementing the senior managers regime	Requests to improve, requiring senior manager attestation that a required improvement has been delivered, higher Pillar 2 capital requirements, and enforcement actions

Source: KPMG research and FSB thematic review on supervisory frameworks and approaches for SIBs (May 2015)

Abbreviations

BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Plan
BIS	Bank for International Settlements
CBK	Central Bank of Kuwait
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organisations of the Treadway Commission
CRD4	Capital Requirements Directive
CRO	Chief Risk Officer
EBA	European Banking Authority
ECB	European Central Bank
EMA	Europe, Middle East, Africa
FCA	Financial Conduct Authority (UK)
FSB	Financial Stability Board
FICC	Fixed Income, Currency and Commodity
FINMA	Swiss Financial Market Supervisory Authority
FX	Foreign Exchange
ICAAP	Internal Capital Adequacy Assessment Process
ILAAP	Internal Liquidity Adequacy Assessment Process
IOSCO	International Organisation of Securities Commissions
PRA	Prudential Regulation Authority
SAMA	Saudi Arabian Monetary Agency
SIB	Systemically Important Bank
SMR	Senior Managers Regime
SREP	Supervisory Review and Evaluation Process

Contact us

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

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

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

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

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

Simon Topping
Principal, Financial Services
Regulatory Center of Excellence
ASPAC region
KPMG International
T: +852 2826 7283
E: simon.topping@kpmg.com

Amy Matsuo
Principal and National Lead
Financial Services Regulatory Risk Practice
KPMG in the US
T: +1 919 380 1509
E: amatsuo@kpmg.com

fsregulation@kpmg.co.uk

www.kpmg.com/regulatorychallenges

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

Designed by Evalueserve.
Publication name: Evolving Banking Regulation – Part Four: Governance: from expectations to delivery
Publication number: 132852-G