TC Notes

Practical leadership & technical guidance from **Toronto Centre**

Improving Corporate Governance in Regulated Firms

JANUARY 2016

Global Affairs Canada
Affaires mondiales Canada
Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY

TORONTOCENTRE
Global Leadership in Financial Supervision

Contents

Introduction[1]

This note explains:

- **the key principles of corporate governance within a regulated financial services firm**
- **why it is important for supervisors to assess standards of corporate governance in the firms they supervise and**
- **how supervisors can improve standards of corporate governance in the firms they supervise.**

This note focuses on corporate governance within regulated financial services firms, in particular the role of the board to set the strategy, policy, culture and values of the firm, and to monitor whether these objectives are being achieved.[2]

The note is relevant to the supervisors of all types of regulated financial institutions, including banking, insurance, securities, financial market infrastructure, and commercial pension companies.

Corporate governance is important for supervisors of regulated firms because:

- Well-managed and well-run financial institutions are less likely to fail, and less likely to treat their customers and counterparties unfairly
- Good corporate governance extends beyond regulatory requirements, and may help to protect depositors, policyholders and investors
- Supervisors can have greater confidence in the internal control mechanisms of firms, and in the information reported to them by firms, when these firms meet high standards of corporate governance, and
- Well-managed and well-controlled firms will be better placed to implement changes in their structure or operations required by supervisors.

Some problems in regulated firms can be traced back to failures of corporate governance, not only ahead of financial crises but also in cases where poor internal controls failed to pick up fraudulent or unauthorised transactions, or where a board failed to control the executive management (or a dominant chief executive).

Supervisors and regulators have a number of tools available to them to improve the standards of corporate governance in the firms they supervise. These include:

- Using international or national standards to set clear expectations for the corporate governance of regulated firms
- Monitoring whether regulated firms meet these expectations, including through on-site reviews
- Introducing an element of individual responsibility and accountability where the boards and senior management of regulated firms are subject to a licensing regime, and
- Taking action when regulated firms fall short of expectations.

[1] This note was prepared by Clive Briault on behalf of Toronto Centre.

[2] This note does not cover in any detail other aspects of corporate governance that are of interest to securities regulators, such as the relationship between a firm and its current and prospective shareholders and bondholders (including the provision by firms of accurate and timely information about their financial performance and ownership; the protection of shareholders' rights; and the equitable treatment of shareholders).

The three annexes to this note summarise (1) key international standards on corporate governance; (2) guidance from international standard-setters on how supervisors should monitor and assess corporate governance in the firms they supervise; and (3) how supervisors should monitor and assess the culture of the firms they supervise.[3]

What is Corporate Governance?

> "*Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined*."[4]

The first "external" part of this description of corporate governance addresses how shareholders can control the actions of the managers of a firm (including through firms providing accurate and timely information about their financial performance and ownership); the rights of shareholders regarding the ownership of a firm, the sale and transfer of shares, voting at shareholder meetings and sharing in the profits of a firm; the equitable treatment of shareholders; and any responsibilities of a firm towards other stakeholders such as employees, customers, and society more generally.[5]

The second, "internal" part of corporate governance relates to how a firm is managed, and to the roles and responsibilities of the board[6] in setting objectives and monitoring performance.

The Key Elements of Internal Corporate Governance

Roles and Responsibilities of the Board:

> To set and guide the strategy, policy, conduct and values of the firm; to establish the framework of risk governance (setting the firm's risk appetite[7], monitoring whether the risks that a firm takes are consistent with this appetite; and identifying, measuring, monitoring, controlling, and reporting all material risks); to set performance objectives and monitor whether they are being achieved; to select key executives and oversee succession planning; to set annual budget and

[3] IOSCO's work on corporate governance has focused predominantly on the issuers of securities rather than on the corporate governance of regulated securities firms. However, the corporate governance of securities firms and financial market infrastructure should be as important to the supervisors of those firms as it is to the supervisors of banks and insurance companies. The Basel Committee and IAIS guidance to supervisors summarised in Annexes 1 and 2 of this note should therefore also be relevant to the supervisors of regulated securities firms.

[4] OECD *Principles of Corporate Governance*, 2015. http://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf

[5] Good corporate governance in this sense may also be important for the health of a country's economy more generally, especially in countries that have moved, or are moving, from state-owned enterprises to market-based ownership structures. Firms have become more dependent on private sources of capital, while the opening up of financial markets has made the allocation of capital among competing purposes, within and across countries, more complex.

[6] In some countries, firms have a unitary board, which contains both executive and non-executive directors. In other countries, firms have a two-tier board structure, in which a supervisory board, consisting entirely of non-executive directors, sits above a management board of executive directors. However, since the roles and responsibilities of unitary and supervisory boards are broadly similar, in this note the term "board" is used to apply to both these types of board. There are also differences across jurisdictions in the scope of board responsibilities and in the liability of individual directors.

[7] The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.

business plans; and to oversee major capital expenditures and acquisitions. To fulfil these responsibilities, boards should have access to timely and relevant management information.

"*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*."[8]

Board Composition and Structure:

Most developed countries expect there to be a majority of non-executives on the boards of major firms, or at least on the key board committees (audit committee and risk committee); a clear division of responsibilities between the chair (or the senior independent director) and the chief executive officer of the firm; an identification of the collective skills required of the board; rigorous and transparent procedures for appointments to the board and for periodic re-appointment; and a regular evaluation of the performance of board members, and of the board as a whole.

Non-Executive Directors:

The primary role of non-executives is to provide both support and constructive challenge to the executive management. This requires non-executives to be sufficiently independent (such as having no prior connection with the firm and no conflicts of interest, and serving for a maximum number of years); to have sufficient experience and expertise; and to commit sufficient time to the role.

Internal Controls:

Boards are generally expected to oversee the establishment of independent and adequately resourced internal control functions to safeguard shareholders' investments and the firm's assets, especially for finance and operational controls, risk management, compliance with the law and relevant standards, and (for insurance firms) an actuarial function.[9] Internal audit (or other internal

[8] UK Prudential Regulatory Authority *Corporate Governance: Board Responsibilities*, Consultation Paper 18/15, May 2015. http://www.bankofengland.co.uk/pra/Documents/publications/cp/2015/cp1815.pdf

[9] In insurance firms the key role of the actuary needs to be explicitly recognised in requirements and guidance on corporate governance. Actuaries play a major role as experts in the risks incurred by the insurer, in controlling the quality of the information the insurer discloses to its owners or participating policyholders and to the supervisory authorities, and in protecting the insured. Most OECD countries require a life insurance company to retain the services of an outside, or in-house, appointed actuary. The actuary should be appropriately qualified in respect of specific professional requirements.

The actuary should undertake an objective assessment of the situation of the insurance company. This requires a degree of independence of the actuary in undertaking this assessment, while at the same time recognising appropriate executive management and board responsibility and accountability. If the actuary is too independent, this might result in the executive management and the board relying too much on the actuary to take decisions and responsibility, while on the other hand a lack of independence of the actuary may increase the discretionary power of executive management.

In some countries, another unique governance issue for insurance companies arises from the discretion that insurance companies may have in their treatment of policyholders; for example, through the operation of with-profits policies. In many countries, the insurance law requires the appointed actuary to make recommendations to

functions, or external review) should then monitor and assess the continuing effectiveness of these internal controls. Control functions, especially internal audit, should not be subject to too much influence of senior management. A direct line of communication to the board is important.

Remuneration:

In many countries the board is responsible for setting the remuneration of the firm's executive management. The board may also have a wider responsibility to oversee the remuneration policies of the firm at all levels to ensure that salary and bonuses reflect long-term profitability and performance, and are consistent with good risk management.

Why is Corporate Governance Important for Supervisors?

The objectives of good corporate governance overlap closely with the objectives of the supervision of financial institutions, since both should contribute to the protection of consumers and investors, to market confidence and to financial stability.

Good corporate governance practices are essential to achieving and maintaining public trust and confidence in the financial system. Financial institutions have a fiduciary responsibility to their customers, which means that good governance is especially important. Poor corporate governance may undermine trust and confidence in the financial system, and may contribute to the failure of financial institutions, or to the mistreatment of consumers and investors.

Good corporate governance also covers a firm's adherence to legislation, regulations, and codes that extend beyond regulation, and which may provide additional protection to consumers, investors, and other stakeholders in the firm.

Moreover, **supervisors can have greater confidence in the internal control mechanisms of financial institutions with high standards of corporate governance**, and in the information reported by such firms. Well-managed and well-controlled financial institutions will also be better placed to implement any changes in their structure or operations required by their supervisors.

This close alignment between good corporate governance and effective financial sector supervision has long been recognised by international standard setters.

Lessons from the Financial Crisis

Poor standards of corporate governance contributed to the financial crisis that emerged in 2007.[10] Poor corporate governance failed to prevent excessive risk-taking in a significant number of financial services firms. The subsequently revealed misconduct (in the setting of interest rate and foreign exchange

---

the board on the distribution of surplus to participating (with-profits) policyholders. Some also require the actuary to give an opinion on the amount that is available for distribution to shareholders.

[10] Lessons from the financial crisis for corporate governance are covered in more detail in:
Grant Kirkpatrick *The Corporate Governance Lessons from the Financial Crisis*, OECD, 2009.
http://www.oecd.org/finance/financial-markets/42229620.pdf
Laura Ard and Alexander Berg *Bank Governance: Lessons from the Financial Crisis*, World Bank Crisis Response Note, March 2010.
http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Note13_Bank_Governance.pdf

benchmarks, and in the treatment of both retail- and wholesale-market customers) in some banks, and other financial institutions, also demonstrates that poor corporate governance failed to create and maintain sufficiently high standards of behaviour at many levels in these firms.

Corporate Governance Failings Evident from the Financial Crisis Included:

- *Boards not exercising adequate oversight of executive management*--insufficient board challenge of executive management, in particular of over-dominant chief executives. In some countries, including the U.S., this was exacerbated when the chief executive was also the chair of the board;
- *Inadequate board understanding of risk*--many boards failed to set a clear risk appetite for the firm, and failed to understand, oversee and control the risks the firm was taking, including the risks arising from an over-expansion into leveraged finance, securitisations and derivatives. Boards (and senior management) relied on management information systems that were unable to aggregate risk exposures across different parts of a firm's business, relied too heavily on models without understanding the limitations of these models, and failed to run adequate stress and scenario tests;[11]
- *Weak non-executive directors*--some boards of financial institutions looked more like a "retirement home for the great and good" than a professional oversight body. Some non-executive directors were appointed because they were personal friends of the chief executive; had no expertise in the financial sector; did not devote enough time to their responsibilities (in some cases because they held too many other directorships); were not sufficiently expert or engaged to understand, monitor and mitigate risk; and did not hold executive management to account through robust challenge;
- *Weak controls*--failure to develop strong internal controls and internal audit capacity;
- *Perverse remuneration incentives*--payment of bonuses to staff that rewarded short-term performance, thereby incentivising excessive risk-taking, without recognising the risks and the longer term performance of the business they conducted; and
- *Culture*--shortcomings in the prevailing culture of banks were an important root cause of continued misconduct and excessive risk-taking.

These problems were not confined to banks. The failure of AIG demonstrated the more general problem of financial institutions moving into new areas of business where the risks and potential downsides were not fully understood by the board, while the problems that emerged in some of the U.S. investment banks demonstrated the problem of poor corporate governance in securities firms.

None of the corporate governance problems revealed by the financial crisis are completely new. Similar problems have emerged across all types of financial institution in the past, including the failure of internal controls to identify rogue traders (Barings); fraud and financial misreporting (BCCI, Refco and Madoff Securities); combining the role of chief actuary and chief executive, and the absence of board understanding of the business (Equitable Life); and over-rapid expansion and the absence of a clear strategy (HIH Insurance Group).

What Should Supervisors Do?

Before the financial crisis that emerged in 2007, **supervisors in some of the most developed international financial markets had relied too heavily on the mantra that the primary responsibility**

[11] This is not to suggest that the boards of financial institutions should have fully predicted or anticipated the financial crisis. But it is the responsibility of non-executive directors to ensure that firms are well run and properly managed, including using stress, and scenario tests to identify vulnerabilities and to decide to what extent the firm should protect itself against these vulnerabilities.

for the safety and soundness of financial institutions rests with the senior management of the regulated firm. The prevailing philosophy of supervision was based on the assumptions that market forces and market discipline would keep regulated firms broadly on track, and that the management and boards of financial institutions had a strong and long-term interest in firms performing well.[12]

The financial crisis undermined both of these assumptions. Supervisors have generally adopted a more intensive and more intrusive approach to supervision. **A closer and tougher supervisory focus on corporate governance in regulated firms needs to be part of this approach**.

Standards

Supervisors need to be clear about the standards of corporate governance, which they expect regulated firms to meet.

Many countries have introduced various forms of legislation, rules, and codes to set and promote high standards of corporate governance.

Legislation typically includes a Companies Act governing the way in which private companies can be established, structured, and operated; legislative requirements on financial reporting and on firms' internal systems and controls; and legislation establishing the criminal nature of fraud, insider dealing, and money laundering.

In addition, many countries have introduced a **national code of corporate governance**.[13] Such codes aim to improve and guide the governance practices of firms within a country's specific legal environment and business context. These national codes may be issued by national stock exchanges, standard-setters for corporate reporting, securities regulators, or other bodies. They generally take the form of non-binding recommendations, typically based on high-level principles, amplified through guidance.

Compliance with codes usually depends on self-regulation and market discipline. Following the model of the United Kingdom, several voluntary codes use the comply-or-explain mechanism. Under this approach, listed companies are required to disclose publicly how they comply with various provisions of the code, or otherwise to explain why they do not comply. Supporters of this approach say that it offers both flexibility and a high degree of compliance. But other commentators say that it is too easy for firms to meet the letter of the code without meeting the spirit of the code, or to explain away any divergences from the code.

Such legislation and codes may not be specific to financial institutions, and they may not cover all regulated firms (for example, national codes of corporate governance typically apply only to firms listed on the stock exchange, although in some countries there are also codes for smaller companies and for state-owned enterprises).

Specific regulatory requirements applying to regulated financial sector firms may therefore be needed, in the form of some combination of high level principles, more detailed rules, and guidance set by the

[12] Clive Briault *Trust less, verify more*, World Bank Crisis Response Note, May 2009. http://documents.worldbank.org/curated/en/2009/07/11077395/trust-less-verify-more

[13] Leading examples of such national codes include the UK Corporate Governance Code (https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf), which evolved from the 1992 Cadbury Code; and the series of King reports in South Africa (https://jutalaw.co.za/uploads/King_III_Report/).

regulator. [14] This will need to be proportional to the size, complexity, structure, and risk profile of the financial institution (for example, systemically important financial institutions should be subject to tougher and more comprehensive standards of corporate governance than smaller firms).

National supervisors and regulators can benefit here from the work of the international standard setters (see Annex 1) and many national financial services regulatory authorities that have **revised their requirements following the financial crisis**. Together, this work covers all types of financial institutions and **emphasises the key elements of corporate governance that were found to have operated inadequately ahead of the financial crisis**. These elements include:

Board Structure and Leadership:

- Effective leadership by the chair of the board in order to encourage and facilitate challenge
- Separating the roles of the chair of the board, and the chief executive officer.

Non-Executive Directors:

- Greater skills, financial industry experience, knowledge of the business and of the business model, and access to critical information
- Adopt more challenging and independent behaviour and culture within the board
- Spend more time in undertaking their role (so hold fewer directorships)
- Ability to seek independent external advice on important decisions.

Risk Governance:

- Explicit board determination and approval of strategy and of risk appetite
- Effectiveness of risk management--identifying, assessing and controlling risks, and embedding a supportive risk culture in the firm
- Establishing a risk committee of the board
- Appointing a chief risk officer (who is independent of business lines) to advise the board on firm-wide risks
- An effective programme of stress and scenario testing, and taking action on the basis of the results--a board should understand the circumstances under which the firm might make a loss, or even fail, and then either be satisfied to take these risks, or put appropriate risk mitigation in place to reduce or remove these risks
- Independent assessments of the firm's risk governance framework, through board effectiveness reviews, internal audit assurance reviews, and third party assessments.

Internal Controls:

- Enhanced resources and independence for internal control functions
- Role of internal audit, and audit committee as key components in how the board gains assurance that internal controls are operating effectively.

[14] For example, in Ireland the financial services regulator introduced specific corporate governance rules for banks and insurance companies: http://www.centralbank.ie/regulation/Documents/Corporate%20Governance%20Requirements%20for%20Credit%20Institutions%202015.pdf and http://www.centralbank.ie/regulation/Documents/Corporate%20Governance%20Requirements%20for%20Insurance%20Undertakings%202015.pdf

Remuneration:

- Board oversight to ensure that remuneration is in line with the desired risk appetite and risk profile of the firm, and consistent with good risk management
- Align remuneration policies with the long-term success of the firm

Culture:

- Role of the board and senior management in establishing, communicating, and assessing the culture, value, and behaviours of the firm
- Board oversight to ensure that staff at all levels are adhering to the culture and values determined by the board

Personal Accountability:

- Assessment of the suitability of board members and senior management
- Holding senior management personally accountable for their firm meeting regulatory requirements and expectations

These revised regulatory requirements represent a gold-standard approach to corporate governance. In practice, supervisors will need to consider how they are going to apply them in a proportional manner to firms that are considerably smaller than the large firms for whom these requirements were primarily designed, to firms that are state-owned[15] or owned by a single, large shareholder[16] (or closely connected shareholders), and to firms in small countries where there is a limited pool of independent, experienced and expert non-executive directors.

Supervision

Supervisors need to monitor whether regulated firms are meeting the required standards of corporate governance.

This can take various forms, and supervisors should consider which of these approaches they need to enhance or introduce. Some of the principles issued by international standard setters include principles directed towards supervisors, covering both what they should be monitoring and assessing, and how they undertake these responsibilities (see Annex 2).

[15] The OECD has issued guidelines for the corporate governance of state-owned enterprises (see Annex 1). These provide internationally agreed standards for how governments should exercise the state ownership function to avoid the pitfalls of both passive ownership and excessive state intervention.

David H. Scott *Strengthening the Governance and Performance of State-Owned Financial Institutions* World Bank Policy Research Working Paper 4321, August, 2007
http://dx.doi.org/10.1596/1813-9450-4321

[16] In some countries, the dominant business model is family owned-and-managed firms. This aligns the interests of management and shareholders much more closely, and in many cases these firms have benefited from a longer-term and more risk-averse approach. But in other cases, family ownership has been associated with a lack of internal challenge and an absence of internal controls, leaving firms exposed to poor decisions and to fraud.

Off-site (desk-based) Analysis

Supervisors can gain some understanding of the corporate governance of a financial institution through off-site analysis, including a review of

- Documentation provided by a financial institution on the structure and composition of the board and its committees; the roles and responsibilities of the board and its committees; the delegation of roles and responsibilities to the chief executive; the operation of the executive management board; and the structure, resourcing and role and responsibilities of internal control functions (risk management, compliance, actuarial, internal audit);
- The minutes of board and board committee meetings and of the meetings of the key internal control committees, which can provide some evidence on how effective the board and these committees are in fulfilling their roles and responsibilities. For example, they may provide some evidence of whether the board has set a clear risk appetite, of whether the board and any board and executive risk committees spend sufficient time discussing, monitoring and controlling risks in an effective and properly informed manner, and of the nature and extent of challenge being made by the non-executive directors;
- Internal reporting from the internal control functions to senior management and the board
- Reports on corporate governance from external auditors and other third parties
- An internal risk and capital adequacy assessment, including an assessment of how a financial institution manages its risks, and the results of the financial institution's own stress and scenario testing. In some countries and in some sectors, financial institutions are required to produce these documents;
- Governance processes in the areas of crisis management and business continuity
- Remuneration policies, the extent of any variable pay, and the extent to which this is subject to constraints (payment in equity rather than cash, deferral of payment and potential claw back); and
- Information on the structure, activities, and group-level oversight processes of the group to which a financial institution belongs.

All these sources can provide supervisors with useful information on basic aspects of corporate governance, such as whether there is a clear separation of roles between the chief executive and the chair of the board, the quality and independence of non-executive directors, the management information received by the board, and the clarity and scope of the firm's strategy and risk appetite documents.

Offsite analysis can also identify concerns and highlight areas of corporate governance that need to be addressed in more detail through onsite examination.

Onsite Assessments:

Onsite assessments are essential for supervisors to obtain more detailed information about corporate governance and to be better able to form judgements about the effectiveness of a financial institution's corporate governance.

Supervisors should explore, through onsite assessments, how corporate governance works in practice within a financial institution, including how the board sets the strategy, culture, and values and risk appetite of the firm; how well members of the board understand the business and its risks; the overall functioning of the board; the nature and extent of challenge by non-executive directors; and how the board seeks and obtains assurance about the quality and effectiveness of the control functions and management information on which it relies.

On-site Assessments Might Include:

- Interviews with non-executive directors (in particular the chair of the board, and the chairs of the audit, risk, and other board committees)
- Interviews with senior management (and, in insurance companies, the chief actuary)
- Interviews with the heads of control functions and the external auditor
- Observing board and executive committee meetings
- Interviews with a range of staff at all levels within a financial institution to assess whether the controls that senior management claims to be in place (and on which the board relies) are really operational throughout the business; and
- A review into how a financial institution manages a particular type of risk (such as credit risk in bank, mortality risk in a life insurance company, the setting of technical provisions in an insurance company, and trading risks in a securities firm), including how such risks are monitored and controlled.

The Purpose of On-site Assessments is to test:

- **Whether the non-executive directors are sufficiently challenging,** or whether there is too cozy a relationship between the non-executives and the chief executive
- How well the board **understands the risks that the firm is running,** and determines the capital, other reserves and provisions, liquidity and other resources required to support these risks
- How well the **board uses information from the firm's external auditors, and from its internal control, and internal audit functions**
- Whether the **core internal control functions are of high quality, sufficiently resourced, and independent of the business**, and
- How the **board assures itself that the firm's internal controls, remuneration, and other policies and procedures operate effectively and are in line with the strategy and risk appetite set by the board**.

However, policies and processes for 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 financial institution's culture, and how to integrate this into their overall risk assessment of the financial institution.[17]

Risk Based Supervision

Many supervisory agencies undertake risk-based supervision.

An assessment of a regulated firm's corporate governance should be a key element of risk-based supervision, because good corporate governance can be an important mitigant against the risks being taken by a financial institution, by lessening the probability that risks will materialise, and by strengthening the ability of a financial institution to manage the impact of those risks if they do materialise. On the other hand, poor corporate governance can magnify the risks that a financial institution is running, making it more likely that risks will materialise, and more likely the consequences of these risks will be severe. Indeed, poor corporate governance is in many respects an additional risk in its own right.

[17] This is discussed in the FSB's *Thematic Review on Supervisory Frameworks and Approaches for SIBs Peer Review Report*, May 2015. http://www.financialstabilityboard.org/wp-content/uploads/Thematic-Review-on-Supervisory-Approaches-to-SIBs.pdf

Risk-based supervision provides a framework for supervisors to assess corporate governance in the wider context of the probability and potential impact of the range of risks that a financial institution is taking. So the assessment of corporate governance is not undertaken in isolation, but takes into account the nature, size, and complexity of the business and other risks relating to each financial institution.

Thematic Reviews

Thematic reviews can be used by supervisors to focus on a specific area of concern, across a sample of financial institutions. This might be done by establishing a team of supervisors to undertake offsite and onsite reviews across a sample of firms, during a period of a few months. The results can then be used to identify good and poor practices across the sample of firms, and to (a) remedy poor practices in the firms where these were identified; (b) promote good practice to all firms by publishing the results, and, when necessary, by amending regulatory rules and guidance; and (c) informing supervisors about what they should be looking for in future firm-specific analysis and visits.

For example, in the area of corporate governance, thematic reviews might include reviews of the expertise and independence of boards, risk governance frameworks, remuneration practices, and specific internal control functions.

Licensing

Some aspects of corporate governance can be addressed as part of a supervisory agency's licensing or authorisation of key individuals (non-executive directors and senior management) in regulated financial institutions. This provides an opportunity for supervisors to (a) evaluate the experience, expertise, and integrity of proposed non-executive directors and senior management, and (b) influence the composition of the board (and of senior management) by refusing to authorise unsuitable candidates.

Until recently, many supervisory agencies only checked that candidates were 'fit and proper' in the sense of there being nothing known against them. However, some supervisory agencies are beginning to take a more active and intensive approach to fit-and-proper assessments of candidates for board and senior management positions, by evaluating their experience and expertise and their suitability for the proposed role. Some supervisory agencies interview candidates as part of the application process, at least for those applying for key roles in large financial institutions.

Corrective Actions

Supervisors need to inform regulated firms of any material weaknesses in corporate governance and require that corrective measures be taken in a timely manner.

This is essentially the same as any other supervisory intervention to change the behaviour of a financial institution, and might include:

- *Negotiation or moral suasion*: Explaining to the financial institution where it falls short of the relevant rules, guidance and other standards, why it is important for the firm to make improvements, and what the consequences will be if these improvements are not made.

- *Supervisory Actions:* Poor corporate governance can be a reason for requiring a financial institution to address the shortcomings directly, or, failing that, to hold additional capital (in particular under the Pillar 2 element of a capital-adequacy regime) or to restrict its business until the shortcomings in corporate governance are rectified.

- *Enforcement Action:* Depending on the powers available to a supervisory agency, and on the enforceability of the specific legislation, rules, and regulations relating to corporate governance, a supervisory agency may be able to address significant failings in corporate governance by imposing fines on the financial institution, or restricting its business, or preventing it from undertaking certain types of business. A supervisory agency may also be able to take action under its fit-and-proper regime to insist on the replacement of individual directors and senior managers.

Resources

Supervisors need to have staff of sufficient quantity, quality and seniority to monitor and assess corporate governance in a regulated firm.

In particular, supervisors need to be sufficiently well-trained, and capable of undertaking onsite examinations and going beyond a 'tick box' approach to exercise judgement about the effectiveness of the corporate governance of a financial institution.

The most important elements are for a supervisor to: (a) understand the relevant national and international codes, standards, and guidance on corporate governance; (b) recognise the difference between "form" and real "substance" in the corporate governance of a financial institution; (c) have the confidence and ability to undertake onsite assessments, including conducting interviews with the directors and senior management of financial institutions; and (d) have the ability to formulate and pursue corrective actions when required.

Powers

Supervisors need to have the authority and the powers to insist that regulated financial institutions improve their corporate governance.

In practice, supervisors may be constrained by a lack of formal powers or authority to (a) issue corporate governance standards; for example, where regulatory requirements are established in legislation (requiring government and/or parliamentary approval) rather than in regulatory rules and guidance; (b) request certain types of information from regulated firms; (c) undertake onsite assessments; or (d) set higher Pillar 2 capital requirements, or impose corrective measures in response to corporate governance failings in regulated firms.

In addition, it is important that supervisors have adequate statutory legal protection against being sued when they have acted in good faith.

Conclusions

Corporate governance is important for all types of financial institutions--banks, insurance and securities companies--and for their supervisors. Poor corporate governance was one contributor to the financial crisis, to serious cases of misconduct, and to a succession of failures of financial institutions.

International standard-setters have revised their various principles covering corporate governance, and new standard-setters such as the Financial Stability Board have entered this arena. There has been a particular focus on the quality and independence of non-executives and the extent to which they challenge executive management; on all aspects of risk governance; on culture; on personal responsibilities and accountability; and on remuneration.

This provides supervisors with a rich set of standards against which to monitor and assess corporate governance in the firms they supervise. But the emphasis of the standards on areas such as

how non-executive directors and boards behave, how boards gain assurance that controls are operating effectively, the quality of management information, and culture means that supervisors will have to rely on onsite assessments using interview and observation techniques with which they may be relatively inexperienced and may lack the confidence to pursue.

Supervisors then need to communicate the shortcomings in corporate governance to firms, and achieve improvements. Actions to rectify shortcomings include supervisory negotiations with financial institutions, the use of additional Pillar 2 capital, and other requirements that will incentivise better corporate governance. Where necessary, supervisors can take disciplinary action against firms and individuals.

Annex 1: Principles of Corporate Governance

The importance of corporate governance, and the search for common standards on which to base IMF and World Bank country assessments, has led to the development of internationally agreed standards and guidelines for corporate governance.

G20/OECD Principles of Corporate Governance (2015)

http://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf

The most important international code is the G20/OECD Principles of Corporate Governance. These Principles were first endorsed by OECD Ministers in 1999, and revised in 2004 and 2015. They have become an international benchmark for policy-makers, investors, corporations, and other stakeholders worldwide. The Principles have been:

- Adopted as one of the Financial Stability Board's (FSB) Key Standards for Sound Financial Systems serving FSB, G20 and OECD members
- Used by the World Bank Group in more than 60 country reviews worldwide, and
- Used as the basis for the Guidelines on the corporate governance of banks issued by the Basel Committee on Banking Supervision, the OECD/IAIS Guidelines on Insurer and Pension Fund Governance, and as a reference point for reform in individual countries.

The Principles focus on publicly traded companies, both financial and non-financial. To the extent they are deemed applicable, they might also be a useful tool to improve corporate governance in companies whose shares are not publicly traded.

The OECD Principles recognise that there is no single model of good corporate governance. However, the OECD has identified some common elements that underlie good corporate governance. The Principles build on these common elements and are formulated to embrace the different models that exist. They apply, regardless of a country's level of ownership concentration, its model of board structure, or whether it has a civil law or a common law tradition.

The OECD Principles are non-binding and do not aim at detailed prescriptions for national legislation. Rather, they seek to serve as a reference point by identifying objectives, and suggesting various means for achieving them. They can be used by national policy-makers as they examine and develop the frameworks for corporate governance that reflect their own economic, social, legal, and cultural circumstances.

The OECD Principles place a strong emphasis on shareholder rights, market efficiency, cost of capital, protecting property rights, and disclosure and transparency. Only the last of the six Principles, which focuses on Board responsibilities, relates to the internal aspects of corporate governance within a firm.

The six Principles (and the most significant revisions introduced in 2015) are:

Principle 1: *Ensuring the basis for an effective corporate governance framework*

This principle focuses on the role of a corporate governance framework in promoting transparent and fair markets, and the efficient allocation of resources. It focuses on the quality and consistency of the different elements of regulations, since these influence corporate governance practices and the division of responsibilities between authorities.

New emphasis is placed on the quality of supervision and enforcement, and on the role of stock markets in supporting good corporate governance.

Principle 2*: The rights and equitable treatment of shareholders and key ownership functions*

This Principle identifies basic shareholder rights, including the right to information and to participation through the shareholder meeting in key company decisions. The chapter also deals with the disclosure of control structures, such as different voting rights.

New issues include the use of information technology at shareholder meetings, the procedures for the approval of related-party transactions, and shareholder participation in decisions on executive remuneration.

Principle 3*: Institutional investors, stock markets and other intermediaries*

This Principle addresses the need for sound economic incentives throughout the investment chain, with a particular focus on institutional investors acting in a fiduciary capacity. It also highlights the need to disclose and minimise conflicts of interest that may compromise the integrity of proxy advisors, analysts, brokers, rating agencies and others who provide analysis and advice that is relevant to investors.

New areas include cross-border listings, and the importance of fair-and-effective price discovery in stock markets.

Principle 4*: The role of stakeholders in corporate governance*

This Principle encourages active co-operation between corporations and their stakeholders, and underlines the importance of recognising the rights of stakeholders that are established by law, or through mutual agreements. It also supports stakeholders' access to information on a timely and regular basis, and their rights to obtain redress for the violations of their rights.

Principle 5*: Disclosure and transparency*

This Principle identifies key areas of disclosure, such as the financial and operating results, company objectives, governance structure and policies, major share ownership, remuneration, related-party transactions, risk factors, and information about board members.

New issues include the recognition of recent trends with respect to items of non-financial information that companies may include on a voluntary basis--for example, in their management reports.

Principle 6: *The responsibilities of the Board*

This Principle provides guidance on the key functions of the board, including the review of corporate strategy, selecting and compensating management, overseeing major corporate acquisitions and divestitures, and ensuring the integrity of the corporation's accounting, financial reporting and other internal control systems. The corporate governance framework should ensure the strategic guidance of the company by the board, the effective monitoring of management by the board, and the board's accountability to the company and its shareholders.
New issues include the role of the board in risk management, tax planning and internal audit; and recommendations on board training and evaluation, and on the establishment of specialised board committees in areas such as remuneration, audit, and risk management.

OECD Guidelines on Corporate Governance of State-Owned Enterprises (2015)

http://www.oecd.org/daf/ca/OECD-Guidelines-Corporate-Governance-SOEs-2015.pdf

These OECD Guidelines recognize the importance of state-owned enterprises (SOEs) in many countries. The Guidelines also recognize the critical importance that the corporate governance of these enterprises has in the overall economic efficiency and competitiveness of the economies concerned.

The Guidelines are recommendations to governments on how to ensure that state-owned enterprises operate efficiently, transparently, and in an accountable manner. The Guidelines were first developed in 2005 as a complement to the OECD Principles of Corporate Governance and were updated in 2015.

These OECD Guidelines cover:

- **The rationale for state ownership**:
  Since the state exercises the ownership of SOEs in the interest of the general public, it should carefully evaluate and disclose the objectives that justify state ownership and subject these to a recurrent review.

- **The state's role as an owner:**
  The state should act as an informed and active owner, ensuring that the governance of SOEs is carried out in a transparent and accountable manner, with a high degree of professionalism and effectiveness.

- **SOEs in the market place:**
  Consistent with the rationale for state ownership, the legal and regulatory framework for SOEs should ensure a level playing field and fair competition in the marketplace when SOEs undertake economic activities.

- **Equitable treatment of shareholders and other investors**:
  Where SOEs are listed or otherwise include non-state investors among their owners, the state and the enterprises should recognise the rights of all shareholders and ensure shareholders' equitable treatment and equal access to corporate information.

- **Stakeholder relations and responsible business**:
  The state ownership policy should fully recognise SOEs' responsibilities towards stakeholders and request that SOEs report on their relations with stakeholders. The policy should make clear any expectations the state has with respect to responsible business conduct by SOEs.

- **Disclosure and transparency:**
  SOEs should observe high standards of transparency and be subject to the same high quality accounting, disclosure, compliance and auditing standards as listed companies.

- **Responsibilities of the board**:
  Boards of SOEs should have the necessary authority, competencies, and objectivity to carry out their functions of strategic guidance and monitoring of management, and should act with integrity and be held accountable for their actions.

FSB Standards on Risk Governance (2013)

http://www.financialstabilityboard.org/wp-content/uploads/r_130212.pdf

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. **These practices focus on risk governance, rather than on corporate governance more generally, and are intended to apply to systemically important regulated firms across all sectors**.

The FSB's sound risk governance practices emphasise the critical role of the board and the board risk committee in *strengthening a financial institution's risk governance, by promoting and evaluating a strong risk culture in the organisation; establishing and communicating the firm's risk appetite; and overseeing management's implementation of the risk appetite and the overall risk governance framework.*

The practices also address the

- 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 chief risk officer (CRO), reporting directly to the chief executive (CEO), not through the chief financial officer (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 (2013)

http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf

The FSB has extended its guidelines on risk governance with two further papers: a set of principles for an effective risk appetite framework, and guidance to supervisors on assessing the risk culture of financial institutions (see Annex 3).

The FSB's Principles for an effective risk appetite framework state that the 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 firm
- 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.

An effective risk appetite framework requires three key elements:

First, a *risk-appetite statement* that:

- Is linked to the firm's short- and long-term strategic, capital and financial plans

- Establishes for each material risk the maximum amount of risk the firm 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 firm bank understands what events might push the firm outside its risk appetite and/or risk capacity.

Second, *risk limits* that:

- Constrain risk-taking within risk appetite
- Are established group-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.

Third, a set of *supporting roles and responsibilities*--the FSB's 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.

Basel Committee Corporate Governance Principles for Banks (2015)

http://www.bis.org/bcbs/publ/d328.pdf

The Basel Committee updated its corporate governance principles in July 2015, replacing the previous version (2010). **The main changes in the new 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.

The thirteen principles are:

Principle 1: *Board's overall responsibilities*

The board has the 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 now 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.

Principle 12: *Disclosure and transparency*

The governance of the bank should be adequately transparent to its shareholders, depositors, other relevant stakeholders and market participants.

Principle 13: *The role of supervisors*

This is covered in Annex 2 below.

Basel Committee Core Principles for effective banking supervision (2012)

http://www.bis.org/publ/bcbs230.pdf

The Basel Core Principles (first issued in 1999 and updated in 2006 and 2012) rely heavily on the internal aspects of corporate governance. A new Core Principle, focused on effective corporate governance as an essential element in the safe and sound functioning of banks, was included in the 2012 revision. The new Principle brings together existing corporate governance criteria in the assessment methodology and gives greater emphasis to sound corporate governance practices.

The Core Principles include:

Core Principle 14: *Corporate governance*

Banks and banking groups should have robust corporate governance policies and processes covering strategic direction, group and organisational structure, control environment, responsibilities of the banks' boards and senior management, and compensation. These policies and processes should be commensurate with the risk profile and systemic importance of the bank.

Core Principle 15*: Risk management process*

Banks should have a comprehensive risk management process (including effective board and senior management oversight) to identify, measure, evaluate, monitor, report and control, or mitigate all material risks on a timely basis; and to assess the adequacy of their capital and liquidity in relation to their risk profile, and market and macroeconomic conditions. This extends to the development and review of contingency arrangements (including robust and credible recovery plans where warranted) that take into account the specific circumstances of the bank. The risk-management process should be commensurate with the risk profile and systemic importance of the bank.

Banks should also have risk-management strategies and policies in place for credit, market, operational, large exposures, country, liquidity, and interest rate risks (as in *Core Principles 17 and 19-25*). These strategies and policies should be reviewed and approved by the board, and implemented effectively.

Core Principle 26: *Internal control and audit*

Banks should have adequate internal control frameworks to establish and maintain a properly controlled operating environment for the conduct of their business, taking into account their risk profile. These include clear arrangements for delegating authority and responsibility; separation of the functions that involve committing the bank, paying away its funds, and accounting for its assets and liabilities; reconciliation of these processes; safeguarding the bank's assets; and appropriate independent internal

audit and compliance functions to test adherence to these controls, as well as applicable laws and regulations.

IAIS/OECD Issues Paper on Corporate Governance (2009)

http://www.oecd.org/dataoecd/43/21/42366179.pdf

In July 2009 the IAIS and the OECD issued jointly an Issues Paper on Corporate Governance. This reflected the growing interest in corporate governance since the IAIS issued its Core Principles in 2003; a joint IAIS/OECD survey in 2008 of current practices and what might represent good practice in the corporate governance of insurance companies; and lessons from the financial crisis.

The Issues Paper discusses the key elements of corporate governance, including:

- Governance structures
- Functions of the board
- Control functions
- Actuarial function
- Disclosure and transparency
- Relations with stakeholders
- Interaction with the supervisor.

IAIS Core Principles (2011, revised 2013 and 2015)

http://iaisweb.org/index.cfm?event=showPage&nodeID=25227

The 2011 update (and subsequent revisions in 2012, 2013 and 2015) of the IAIS's Core Principles develops further the issues identified in the IAIS/OECD 2009 issues paper.

Core Principle 7: *Corporate Governance*

The supervisor requires insurers to establish and implement a corporate governance framework, which provides for sound and prudent management and oversight of the insurer's business, and adequately recognises and protects the interests of policyholders.

The supervisor should therefore require the insurer to demonstrate the adequacy and effectiveness of its corporate governance framework; and require the insurer's board to:

- Set and oversee the implementation of the insurer's corporate culture, business objectives, and strategies for achieving those objectives, including its risk strategy and risk appetite, in line with the insurer's long term interests and viability
- Provide oversight of the design and implementation of sound risk management and internal controls
- Have an appropriate number and mix of individuals to ensure that there is an overall adequate level of competence at the board level commensurate with the governance structure and the nature, scale and complexity of the insurer's business
- Ensure that board members act in good faith, honestly and reasonably, exercise due care and diligence, act in the best interests of the insurer and policyholders, exercise independent judgment and objectivity, and do not use their position to gain undue personal advantage

- Have appropriate internal governance practices and procedures to support the work of the board in a manner that promotes the efficient, objective and independent judgment and decision making by the board
- Have adequate powers and resources to be able to discharge its duties fully and effectively
- Ensure that the roles and responsibilities allocated to the board, senior management and key persons in control functions are clearly defined so as to promote an appropriate separation of the oversight function from the management responsibilities, and provide adequate oversight of the senior management
- Have appropriate policies and procedures to ensure that senior management carries out the day-to-day operations of the insurer effectively and in accordance with the insurer's strategies, policies and procedures; promotes a culture of sound risk management, compliance and fair treatment of customers; provides the board adequate and timely information to enable the Board to carry out its duties and functions including the monitoring and review of the performance and risk exposures of the insurer, and the performance of senior management; and provides to the relevant stakeholders and the supervisor the information required to satisfy legal and other obligations;
- Adopt and oversee the effective implementation of a written remuneration policy which does not induce excessive or inappropriate risk-taking, is in line with the corporate culture, objectives, strategies, identified risk appetite and long term interests of the insurer, has proper regard to the interests of its policyholders and other stakeholders, and covers at a minimum, individuals who are members of the board, senior management, key persons in control functions and other employees whose actions may have a material impact on the risk exposure of the insurer; and
- Ensure there is a reliable financial reporting process for both public and supervisory purposes, which is supported by clearly defined roles and responsibilities of the board, senior management and the external auditor, and that there is adequate governance and oversight of the external audit process.

Core Principle 8: *Risk Management and Internal Controls*

An insurer should have, as part of its overall corporate governance framework, effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters, and internal audit.

IOSCO Objectives and Principles of Securities Regulation (2010)

https://www.iosco.org/library/pubdocs/pdf/IOSCOPD323.pdf

https://www.iosco.org/library/pubdocs/pdf/IOSCOPD359.pdf

The IOSCO Objectives and Principles of Securities Regulation (first published in 2003 and updated in 2008 and 2010) and the accompanying methodology for assessing implementation (2011, revised in 2013) set out in detail the external aspects of corporate governance under the Principles relating to issuers of securities. These external aspects relate to all firms that issue securities, not specifically to financial institutions.

These three Principles are:

Principle 16: There should be full, accurate, and timely disclosure of financial results, risk and other information which is material to investors' decisions.

Principle 17: Holders of securities in a company should be treated in a fair and equitable manner. This Principle addresses many of the same issues that are covered by Principles 1 and 2 of the OECD Principles of Corporate Governance regarding the rights and equitable treatment of shareholders.

Principle 18: Accounting standards used by issuers to prepare financial statements should be of a high and internationally acceptable quality.

However, the IOSCO Principles contain relatively little material on the internal aspects of the corporate governance of regulated securities firms. The key Principle here is:

Principle 31: Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, with the aim of protecting the interests of clients and their assets, and ensuring proper management of risk, through which management of the intermediary accepts primary responsibility for these matters.

Annex 2: Supervision

Basel Committee Corporate Governance Principles for Banks (2015)

http://www.bis.org/bcbs/publ/d328.pdf

Principle 13 of the Basel Committee Corporate Governance Principles states that supervisors should:

- **Provide guidance for and supervise corporate governance at banks, including through comprehensive evaluations and regular interaction with boards and senior management**
- **Require improvement and remedial action as necessary, and**
- **Share information on corporate governance with other supervisors**.

Principle 13 provides additional guidance to supervisors covering each element of this Principle.[18]

Guidance on expectations for sound corporate governance

Supervisors should establish guidance, or rules requiring banks to have robust corporate governance policies and practices. Such guidance is especially important where national laws, regulations, codes, or listing requirements regarding corporate governance are not sufficiently robust to address the unique corporate governance needs of banks.

Guidance for banks should address, among other things, expectations for checks and balances and a clear allocation of responsibilities, accountability and transparency among the members of the board and senior management, and within the bank.

In addition to guidance or rules, where appropriate, supervisors should also share industry best practices regarding corporate governance with the banks they supervise.

Assessment

Supervisors should have processes in place to evaluate a bank's corporate governance. Such evaluations may be conducted through regular reviews of written materials and reports, interviews with

[18] The detail of Basel Committee Core Principle 14 on corporate governance contains similar guidance for supervisors.

board members and bank personnel (including senior management, those responsible for the risk, compliance and internal audit functions, and external auditors), examinations, self-assessments by the bank, and other types of onsite and offsite monitoring.

Supervisors should evaluate whether the bank has in place effective mechanisms through which the board and senior management execute their respective oversight responsibilities, including oversight of the bank's strategic objectives, risk appetite, financial performance, capital adequacy, capital planning, liquidity, risk profile and risk culture, controls, compensation practices, and the selection and evaluation of management.

Supervisors should focus particular attention on the oversight of the risk management, compliance, and internal audit functions. This should include assessing the extent to which the board interacts with these functions. Supervisors should determine whether internal controls are being adequately assessed and contribute to sound governance throughout the bank.

Supervisors should evaluate the processes and criteria used by banks in the selection of board members and senior management and, as they judge necessary, obtain information about the expertise and character of board members and senior management. The fit and proper criteria should include those discussed in Principle 2 (see Annex 1 above). The individual and collective suitability of board members and senior management should be subject to ongoing attention by supervisors.

Supervisors should also endeavour to assess the governance effectiveness of the board and senior management, especially with respect to the risk culture of the bank.

An assessment of governance effectiveness aims to determine the extent to which the board and senior management demonstrate effective behaviours that contribute to good governance. This assessment includes a supervisory review of any board and management assessments, surveys and other information, as well as supervisory interviews, observations and qualitative judgments. In arriving at such judgments, supervisors need to be particularly mindful of consistency of treatment across the banks they supervise. Supervisory staff should have the necessary skills to evaluate these issues and arrive at the complex judgments involved in assessing governance effectiveness.

An assessment of culture should include consideration of the behavioural dynamic of the board and senior management, such as how the "tone at the top" and the cultural values of the bank are communicated and put into practice, how information flows to and from the board and senior management, and how potentially serious problems are identified and addressed throughout the organisation. (See also Annex 3 below)

In reviewing corporate governance in the context of a group structure, supervisors should take into account the corporate governance responsibilities of both the parent company and its subsidiaries.

Regular interaction with directors and senior management

Supervisors should interact regularly with boards of directors, individual board members, senior managers and those responsible for the risk management, compliance and internal audit functions. This should include scheduled meetings and ad hoc exchanges. The purpose of these interactions is to support timely and open dialogue between the bank and its supervisors on a range of issues, including the bank's strategies, business model and risks; the effectiveness of corporate governance; the bank's culture; management issues; succession planning; and compensation and incentives.

The frequency of these interactions may vary according to the size, complexity, structure, economic significance and risk profile of the bank. On that basis, supervisors may, for example, meet with the full board of directors annually, but more frequently, with the chairman, lead or senior independent director, and with key committee chairs. For systemically important banks, interaction should occur more frequently, particularly with members of the board and senior management, and those responsible for the risk management, compliance and internal audit functions.

Requiring improvement and remedial action by a bank

Supervisors should have a range of tools at their disposal to address governance improvement needs and governance failures. Supervisors should raise corporate governance issues with the bank, and should provide insights to the bank on its operations relative to its peers, market developments and emerging systemic risks.

Supervisors should be able to require steps towards improvement and remedial action, and ensure accountability for the corporate governance of a bank. These tools may include the ability to compel changes in the bank's policies and practices, the composition of the board of directors or senior management, or other corrective actions. They should also include, where necessary, the authority to impose sanctions or other punitive measures. The choice of tool and the time frame for any remedial action should be proportionate to the level of risk the deficiency poses to the safety and soundness of the bank, or the relevant financial system(s).

When a supervisor requires a bank to take remedial action, the supervisor should set a timetable for completion. Supervisors should have escalation procedures in place to require more stringent or accelerated remedial action in the event that a bank does not adequately address the deficiencies identified, or the supervisor deems that further action is warranted.

Share information on corporate governance with other supervisors

Cooperation and appropriate information sharing among relevant public authorities, including bank supervisors and conduct authorities, can significantly contribute to the effectiveness of these authorities in their respective roles. Such information sharing is particularly important between home and host supervisors of cross-border banking entities, and can help supervisors improve their assessment of the overall governance of a bank and the risks it faces, particularly in a group context, and help other authorities assess the risks posed to the broader financial system.

IAIS Core Principles (2011, revised 2013 and 2015)

http://iaisweb.org/index.cfm?event=showPage&nodeID=25227

IAIS Core Principle 9 states that supervisors should take a risk-based approach to supervision that uses both off-site monitoring and on-site inspections to examine the business of each insurer, evaluate its condition, risk profile and conduct, the quality and effectiveness of its corporate governance and its compliance with relevant legislation and supervisory requirements. The supervisor should obtain the necessary information to conduct effective supervision of insurers and evaluate the insurance market.

An evaluation of the effectiveness of the corporate governance framework, including its risk management and internal control systems, can be undertaken through:

- Reviewing and analysing the minutes of the board and its committees, the auditors' reports and, if any, actuaries' and electronic data processing audits
- Analysing the ownership structure and sources of capital funds

- Evaluating the independence of the board members, the suitability (fitness and propriety) of the board members, senior management and key persons in control functions, their effectiveness, and their ability to acknowledge improvement needs and correct mistakes (especially after such needs or mistakes have been identified by the insurer, its auditors, or the supervisor and after changes of management and in the board)
- Examining the insurer's internal policies, processes and controls in order to assess the adequacy of these in light of the insurer's risk profile
- Examining the accounting procedures in order to assess the accuracy of the financial and statistical information periodically sent to the supervisor, and its compliance with the regulations, and
- Evaluating the organisation and the management of the insurer.

IAIS/OECD Issues Paper on Corporate Governance (2009)

http://www.oecd.org/dataoecd/43/21/42366179.pdf

The IAIS/OECD Issues Paper on Corporate Governance includes some guidance on the role of supervisors in assessing the governance of insurers, including the importance of supervisors:

- Determining whether the insurer has adopted and effectively implemented sound corporate governance policies and practices;
- Assessing the fitness and propriety of board members
- Monitoring the performance of boards (for example, reading minutes of boards and committees, asking challenging questions, and establishing supervisory expectations)
- Assessing the functioning of the board as a whole, including the overall functioning of the board and board dynamics
- Assessing the adequacy of governance processes in the area of crisis management and business continuity
- Assessing the quality of insurers' internal reporting, risk management, audit and control functions
- Evaluating the effects of the insurer's group structure, and
- Bringing to the attention of the board and senior management problems that they detect through their supervisory activities, while taking care to ensure that the board does not rely on the supervisory authority to assess its corporate governance.

The Issues Paper emphasises that supervisors need to have staff of sufficient quantity, quality and seniority to monitor and assess an insurance company's performance in the area of corporate governance.

European Banking Authority SREP Guidelines (2014)

http://www.eba.europa.eu/documents/10180/935249/EBA-GL-2014-13+%28Guidelines+on+SREP+methodologies+and+processes%29.pdf

Supervisors are expected to cover the following areas relating to corporate governance in their risk assessment of a bank:

Organisation and functioning of the board: The board has an adequate number and composition of members, who are fit and proper, and demonstrate a sufficient level of commitment and independence; there are effectiveness reviews of the board, and 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: The framework considers all material risks to which the bank is exposed and contains risk limits consistent with the bank's risk appetite; it is forward-looking, in line with the strategic planning horizon, and regularly reviewed; and stress testing is embedded in the framework, with board and senior management involved, and integrated into decision-making.

Internal control framework: The first line (business units) of defence is responsible in the first instance for establishing and maintaining adequate internal controls. There are independent second (risk and compliance) and third (internal audit) lines of defence; a clear allocation of responsibilities; policies and procedures to identify, measure, monitor, mitigate and report risk; risk control functions are 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; and there is a CRO with a sufficient mandate and independence.

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

Remuneration: Remuneration policy is 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; and includes an appropriate combination of variable and fixed remuneration.

Annex 3: Culture

FSB Guidance to supervisors on assessing the risk culture of financial institutions (2014)

http://www.financialstabilityboard.org/wp-content/uploads/140407.pdf

The FSB's Guidance on assessing risk culture is intended to help supervisors to understand a financial institution'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 financial institution's risk appetite framework; and on whether the financial institution's risk culture supports adherence to the agreed risk appetite and to sound risk management.

The FSB expects **supervisors to focus on four, key risk culture indicators**, to look in particular for behaviours or attitudes that are not supportive of sound risk management, and to intervene early to address the potential build-up of excessive risk. The four indicators of a good culture are:

Tone from the top--how the financial institution's leadership sets the core values and expectations, and ensures that these 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 financial institution, ensuring common understandings of risk, and learning from risk culture failures.

Accountability: All employees know the core values and expectations, and know as well, that the consequences of the failure to uphold them will be enforced--a clear allocation of risk ownership, escalation processes, and internal enforcement procedures.

Effective challenge: Decision-making considers a range of views, practices are tested, and open discussion is encouraged--encouraging challenge and dissent, and organising the risk functions to provide access to senior management and the board.

Incentives: The financial and non-financial compensation that is available to all levels of employees, rewards the behaviours that support the core values and expectations, basing remuneration on adherence to risk appetite, and to desired cultures and behaviours, and appropriate talent development and succession planning.

Basel Committee Corporate Governance Principles for banks (2015)

http://www.bis.org/bcbs/publ/d328.pdf

The revised Basel Committee corporate governance principles include some guidelines on culture.

Fundamentals: A corporate culture that reinforces appropriate norms for responsible and ethical behaviour is a fundamental component of good governance. These norms are especially critical in terms of a bank's risk culture--its risk awareness, risk-taking behaviour and risk management.

Tone at the top: To promote a sound corporate culture, the board should:

- Set corporate values that create expectations that all business should be conducted in a legal and ethical manner
- Confirm that appropriate steps have been, or are being taken to communicate throughout the organisation the corporate values, professional standards or codes of conduct it sets, together with supporting policies
- Oversee the adherence to such values by senior management and other employees
- Confirm that employees, including senior management, are aware that appropriate disciplinary or other actions will follow unacceptable behaviours and transgressions, and
- Promote risk awareness within a strong risk culture, conveying the board's commitment that it does not support excessive risk-taking and that all employees are responsible for helping the financial institution operate within the established risk appetite and risk limits.

Code of conduct: A code of conduct (or code of ethics, or comparable policy) should define acceptable and unacceptable behaviours. It should explicitly disallow illegal activity, and it should make clear that employees are expected to conduct themselves ethically, and perform their job with skill and due care and diligence, in addition to complying with laws, regulations and company policies.

Effective challenge: A firm's corporate values should recognise the critical importance of timely and frank discussion, and the communication of problems to higher levels within the organisation:

- Employees should be encouraged and able to communicate, confidentially and without the risk of reprisal, legitimate concerns about illegal, unethical or questionable practices, including communicating material concerns to the financial institution's supervisor

- The board should have oversight of the whistleblowing policy mechanism, to ensure that senior management addresses legitimate issues that are raised, and that staff who raise concerns are protected from detrimental treatment or reprisals, and
- The board should oversee and approve how, and by whom, legitimate material concerns are investigated and addressed.

EBA SREP Guidelines (2014)

http://www.eba.europa.eu/documents/10180/935249/EBA-GL-2014-13+%28Guidelines+on+SREP+methodologies+and+processes%29.pdf

Supervisors are expected to include in their risk assessment whether:

- The financial institution has a sound corporate and risk culture that is adequate for the scale, complexity, and nature of its business, and is based on sound, clearly expressed values that take into account the institution's risk appetite
- The board sets governance principles, corporate values and appropriate standards, including independent whistle-blowing processes and procedures
- The financial institution's ethical, corporate and risk culture creates an environment of effective challenge in which decision-making processes promote a range of views, and
- There is evidence of clear and strong communication of strategies and policies to all relevant staff, and that the risk culture is applied across all levels of the institution.