FSB FINANCIAL STABILITY BOARD

Thematic Review on Risk Governance

Peer Review Report

12 February 2013

Thematic Review on Risk Governance

Peer Review Report

Table of Contents

Annexes

Foreword

Financial Stability Board (FSB) member jurisdictions have committed, under the FSB Charter and in the *FSB Framework for Strengthening Adherence to International Standards*,[1] to undergo periodic peer reviews. To fulfil this responsibility, the FSB has established a regular programme of country and thematic peer reviews of its member jurisdictions.

Thematic reviews focus on the implementation and effectiveness across the FSB membership of international financial standards developed by standard-setting bodies and policies agreed within the FSB in a particular area important for global financial stability. Thematic reviews may also analyse other areas important for global financial stability where international standards or policies do not yet exist. The objectives of the reviews are to encourage consistent cross-country and cross-sector implementation; to evaluate (where possible) the extent to which standards and policies have had their intended results; and to identify gaps and weaknesses in reviewed areas and to make recommendations for potential follow-up (including via the development of new standards) by FSB members.

This report describes the findings of the thematic peer review on risk governance, including the key elements of the discussion in the FSB Standing Committee on Standards Implementation (SCSI). The draft report for discussion was prepared by a team chaired by Swee Lian Teo (Monetary Authority of Singapore), comprising Ted Price (Canada Office of the Superintendent of Financial Institutions), Xiang Qi (China Banking Regulatory Commission), Jérôme Lachand (France Autorité de Contrôle Prudentiel), Sofia Nikopoulos (German BaFin), Adriana Elizondo (Mexico National Banking and Securities Commission), Francisco Gil (Bank of Spain), Mike Brosnan (United States Office of the Comptroller of the Currency), Xavier-Yves Zanota (member of the Basel Committee on Banking Supervision Secretariat), Mats Isaksson (Organisation for Economic Co-operation and Development), and Laura Ard (World Bank). Merylin Coombs and Grace Sone (FSB Secretariat) provided support to the team and contributed to the preparation of the peer review report.

[1] See http://www.financialstabilityboard.org/publications/r_100109a.pdf.

Glossary

Definitions often differ across jurisdictions. For purposes of this peer review, the following definitions are used:

Audit committee:	A specialised board-level committee that is charged with oversight of the organisation's audit function.
Board of directors or board:	The structure of the board differs between countries.[2] The use of "board" throughout the paper encompasses the different national models that exist and refers to the oversight function and general management function of the financial institution and should be interpreted in accordance with national circumstances.
Executive director:	A member of the board (e.g., director) who also has management responsibilities within the firm.
Independent director:	The use of "independent" throughout this paper refers to a member of the board who does not have any management responsibilities with the firm and is not under any other undue influence that would impede the director's exercise of objective judgement.
Non-executive director:	A member of the board who does not have management responsibilities within the firm.
Risk appetite:	The aggregate level and types of risk a firm is willing to assume in its exposures and business activities in order to achieve its business objectives.
Risk appetite framework:	The framework of policies and processes that establish and monitor adherence to the firm's risk appetite.
Risk appetite statement:	An outline of the aggregate levels and types of risk a firm is willing to accept to achieve its business objectives.
Risk capacity:	The maximum level of risk the firm can assume before it breaches regulatory constraints (e.g., capital, liquidity) or other stakeholders' constraints (e.g., dividend pay-out).

[2] As noted in the BCBS 2010 *Principles for enhancing corporate governance*, some countries use a two-tier structure, where the supervisory function of the board is performed by a separate entity known as a supervisory board, which has no executive functions. Other countries, by contrast, use a one-tier structure in which the board has a broader role. Still other countries have moved or are moving to an approach that discourages or prohibits executives from serving on the board or limits their number and/or requires the board and its committees to be chaired only by non-executive board members. Owing to these differences, this document does not advocate a specific board structure. The term board refers to the oversight function and the management function in general and should be interpreted throughout the document in accordance with the applicable law within each jurisdiction. The same applies to the committees mentioned in this report which may be under the control of different board functions, accordingly, subject to the board structure and subject to the respective tasks. Recognising that different structural approaches to corporate governance exist across countries, this document encourages practices that can strengthen checks and balances and sound risk governance under diverse structures.

Risk committee: A specialised board-level committee charged with oversight of risk at the institution, including of the risk management function, and is responsible for advising the board on the firm's overall current and future risk appetite and risk strategy, and for overseeing the implementation of that strategy.

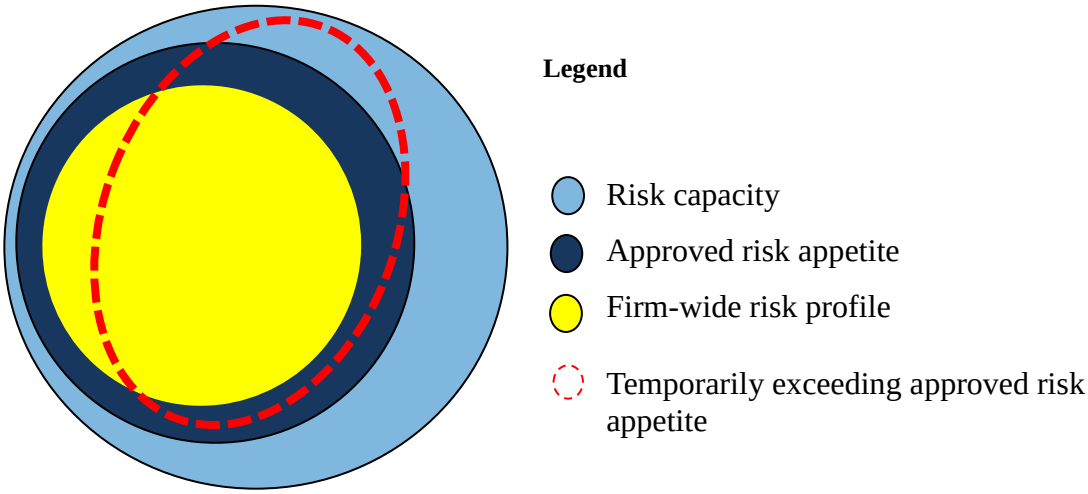
Risk governance framework: The framework through which the board and management establish the firm's strategy; articulate and monitor adherence to risk appetite and risk limits; and identify, measure and manage risks.

Risk limits: The allocation of the firm's risk appetite statement to:

- specific risk categories (e.g., credit, market, liquidity, operational);
- the business unit or platform level (e.g., retail, capital markets);
- lines of business or product level (e.g., concentration limits, value-at-risk, or VaR, limits); and
- other levels, as appropriate.

Risk profile: A point in time assessment of the firm's risk exposures.

Chart 1: Illustration of terms used in risk appetite statements



A firm's risk appetite should be set below the risk capacity of the firm so that a buffer exists between risk capacity and risk appetite. The firm-wide risk profile (comprises individual business unit risks) should be measured, monitored and managed to ensure that the firm's overall risk stays within specified risk limits. A firm generally sets risk limits that will constrain risk within its approved risk appetite. Some business units/lines may exceed the risk limits set and no longer operate within the approved risk appetite. Breaches in risk limits should be reported to the board or risk committee and management should propose actions to reduce the risk of the business unit/line to within the approved risk appetite.

Executive summary

The recent global financial crisis exposed a number of governance weaknesses that resulted in firms' failure to understand the risks they were taking. In the wake of the crisis, numerous reports painted a fairly bleak picture of risk governance frameworks at financial institutions, which consists of the three key functions: the board, the firm-wide risk management function, and the independent assessment of risk governance. The crisis highlighted that many boards had directors with little financial industry experience and limited understanding of the rapidly increasing complexity of the institutions they were leading. Too often, directors were unable to dedicate sufficient time to understand the firm's business model and too deferential to senior management.

In addition, many boards did not pay sufficient attention to risk management or set up effective structures, such as a dedicated risk committee, to facilitate meaningful analysis of the firm's risk exposures and to constructively challenge management's proposals and decisions. The risk committees that did exist were often staffed by directors short on both experience and independence from management. The information provided to the board was voluminous and not easily understood which hampered the ability of directors to fulfil their responsibilities. Moreover, most firms lacked a formal process to independently assess the propriety of their risk governance frameworks. Without the appropriate checks and balances provided by the board, the risk management function, and independent assessment functions, a culture of excessive risk-taking and leverage was allowed to permeate in these weakly governed firms. Further, with the risk management function lacking the authority, stature and independence to rein in the firm's risk-taking, the ability to address any weaknesses in risk governance identified by internal control assessment and testing processes was obstructed.

The peer review found that, since the crisis, national authorities have taken several measures to improve regulatory and supervisory oversight of risk governance at financial institutions. These measures include developing or strengthening existing regulation or guidance, raising supervisory expectations for the risk management function, engaging more frequently with the board and management, and assessing the accuracy and usefulness of the information provided to the board to enable effective discharge of their responsibilities. Nonetheless, more work remains; national authorities need to strengthen their ability to assess the effectiveness of a firm's risk governance, and more specifically its risk culture to help ensure sound risk governance through changing environments. Supervisors will need to undergo a substantial change in approach since assessing risk governance frameworks entails forming an integrated view across all aspects of the framework.

The peer review also asked supervisors to evaluate progress made by their surveyed firm(s) toward enhanced risk governance in seven areas.[3] To provide some consistency to this exercise, the review team developed high-level criteria to assist supervisory evaluations of

[3] Supervisors were provided high-level criteria to evaluate firms' progress toward enhancing risk governance in the following areas:
(i) firm's approach toward risk governance;
(ii) defined responsibilities for the board;
(iii) defined responsibilities for the risk committee;
(iv) governance of the board and risk committee;
(v) information provided to the board and risk committee;
(vi) risk management function; and
(vii) independent assessment of the risk management function.

firms' progress, drawing from a compilation of relevant principles, recommendations and supervisory guidance. The high-level criteria were viewed as fundamental prerequisites for risk governance frameworks. This evaluation found that many of the best risk governance practices at surveyed firms are now more advanced than national guidance. This outcome may have been motivated by firms' need to regain market confidence rather than regulatory requirements. Firms have made particular progress in:

- assessing the collective skills and qualifications of the board as well as the board's effectiveness either through self-evaluations or through the use of third parties;
- instituting a stand-alone risk committee that is composed only of independent directors and having a clear definition of independence;
- establishing a group-wide chief risk officer (CRO) and risk management function that is independent from revenue-generating responsibilities and has the stature, authority and independence to challenge decisions on risk made by management and business lines; and
- integrating the discussions among the risk and audit committees through joint meetings or cross-membership.

Although many surveyed firms have made progress in the last few years, significant gaps remain, relative to the criteria developed, particularly in risk management. There were also differences in progress across regions with firms in advanced economies having adopted more of the desirable risk governance practices.

The results of the supervisory evaluations were grouped by: (i) all surveyed firms; (ii) firms identified by the FSB and Basel Committee on Banking Supervision (BCBS) as global systemically important financial institutions, or G-SIFIs[4]; and (iii) firms that reside in advanced economies (AEs) or emerging market and developing economies (EMDEs)[5]. In summary, across the seven areas evaluated, firms have made the most progress in defining the board's role and responsibilities, and reasonable progress in their approach to risk governance and the independent assessment of risk governance. The supervisory evaluations, however, indicate that surveyed firms should continue to work toward defining the responsibilities of the risk committee and strengthening their risk management functions as nearly 50 per cent of surveyed firms did not meet all of the evaluation criteria in these areas. By type of institution, surveyed G-SIFIs are more advanced than other financial institutions in defining the responsibilities of the board and risk committee, conducting independent assessments of risk governance, providing relevant information to the board and risk committee, and to some extent more advanced in the risk management function. These results support the finding that the firms in the regions hardest hit by the financial crisis have made the most progress. Meanwhile, supervisory evaluations of firms that reside in EMDEs show that nearly 65 per cent did not meet all of the criteria for the risk management function. These gaps need immediate attention by both supervisors and firms.

---

[4] See the FSB update on the group of global systemically important banks (G-SIBs) issued on 1 November 2012 at: http://www.financialstabilityboard.org/publications/r_121031ac.pdf.

[5] The classification of firms by Advanced Economies and Emerging Market and Developing Economies is based on the World Bank World Development Indicators.

Other significant findings coming out of the review include the following:

- National authorities do not engage on a sufficiently regular and frequent basis with the board, risk committee and audit committee. Several jurisdictions hold such meetings only once a year or on an as-needed basis.
- Good progress has been made toward elevating the CRO's stature, authority, and independence. In many firms, the CRO has a direct reporting line to the chief executive officer (CEO) and a role that is distinct from other executive functions and business line responsibilities (e.g., no "dual-hatting").[6] This elevation, however, needs to be supported by the involvement of the risk committee in reviewing the performance and setting the objectives of the CRO, ensuring that the CRO has access to the board and risk committee without impediment (including reporting directly to the board/risk committee), and facilitating periodic meetings with directors without the presence of executive directors or other management.
- More work is needed on the part of both national authorities and firms on establishing an effective risk appetite framework (RAF). Assessing a firm's RAF is a challenging task that requires greater clarity and an elevated level of consistency among national authorities.
- Supervisory expectations for the independent assessment of internal control systems by internal audit or other independent function were well-established prior to the crisis. As such, this is an area that demonstrated relatively sound practices across the FSB membership at both national authorities and firms. However, no jurisdiction had specific expectations for internal audit to periodically provide a firm-wide assessment of risk management or risk governance processes.
- Nearly all firms have an independent chief audit executive (CAE) who reports administratively to the CEO and the audit committee chair and who directly reports audit findings to a permanent audit committee. However, there is still room for improving the CAE's access to directors beyond those on the audit committee.

Drawing from the findings of the review, including discussions with industry organisations as well as risk committee directors and CROs of several firms that participated in the review, the report identifies some of the better practices exemplified by national authorities and firms to collectively form a list of sound risk governance practices (see Section V). It also draws on some of the relevant principles and recommendations for risk governance published by other organisations and standard setting bodies. No one single authority or firm, however, demonstrated all of these sound practices. This integrated and coherent list of sound practices aims to help national authorities take a more holistic approach to risk governance, rather than looking at each facet in isolation, and may provide a basis for consideration by authorities and standard setting bodies as they review their guidance and standards for strengthening risk governance practices.

[6] For instance, the CRO reporting to the chief financial officer (CFO) or assuming the responsibilities of both the CRO and CFO should be avoided to preserve the independence and effectiveness of both roles.

The review sets out several recommendations to ensure the effectiveness of risk governance frameworks continue to improve by targeting areas where more substantial work is needed. While the review focused on banks and broker-dealers that are systemically important, these recommendations apply to other types of financial institutions, including insurers and financial conglomerates.

Recommendations:

1. To ensure that firms' risk governance practices continue to improve, FSB member jurisdictions should strengthen their regulatory and supervisory guidance for financial institutions, in particular for SIFIs, and devote adequate resources (both in skills and quantity) to assess the effectiveness of risk governance frameworks. In particular, national authorities should consider the following sound risk governance practices:

    i. set requirements on the independence and composition of boards, including requirements on relevant types of skills that the board, collectively, should have (e.g., risk management, financial industry expertise) as well as the time commitment expected.

    ii. hold the board accountable for its oversight of the firm's risk governance and assess if the level and types of risk information provided to the board enable effective discharge of board responsibilities. Boards should satisfy themselves that the information they receive from management and the control functions is comprehensive, accurate, complete and timely to enable effective decision-making on the firm's strategy, risk profile and emerging risks. This includes establishing communication procedures between the risk committee and the board and across other board committees, most importantly the audit and finance committees.

    iii. set requirements to elevate the CRO's stature, authority, and independence in the firm. This includes requiring the risk committee to review the performance and objectives of the CRO, ensuring the CRO has unfettered access to the board and risk committee (including a direct reporting line to the board and/or risk committee), and expecting the CRO to meet periodically with directors without executive directors and management present. The CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities (e.g., no "dual-hatting"). Further, the CRO should be involved in activities and decisions (from a risk perspective) that may affect the firm's prospective risk profile (e.g., strategic business plans, new products, mergers and acquisitions, internal capital adequacy assessment process, or ICAAP).

    iv. require the board (or audit committee) to obtain an independent assessment of the design and effectiveness of the risk governance framework on an annual basis.

v. engage more frequently with the board, risk committee, audit committee, CEO, CRO, and other relevant functions, such as the CFO, to assess the firm's risk culture (e.g., the "tone at the top"), whether directors provide effective challenge to management's proposals and decisions, and whether the risk management function has the appropriate authority to influence decisions that affect the firm's risk exposures.

2. The relevant standard setting bodies (e.g., BCBS, IAIS, IOSCO, OECD) should review their principles for governance, taking into consideration the sound risk governance practices listed in Section V.

3. Risk culture plays a critical role in ensuring effective risk governance endures through changing environments. The FSB Supervisory Intensity and Effectiveness group has agreed to implement the recommendation from the 2012 FSB progress report on enhanced supervision to explore ways to formally assess risk culture, particularly at G-SIFIs. This work should be completed by September 2013.

4. To improve their ability to assess firms' progress toward more effective risk management, national authorities should provide guidance on the key elements that are incorporated in effective risk appetite frameworks. To enable firms to define frameworks with a minimum amount of comparability despite their firm-specific nature, a common nomenclature for terms used in risk appetite statements (e.g., "risk appetite", "risk capacity", "risk limits") should be established. The FSB Supervisory Intensity and Effectiveness group, in collaboration with relevant standard setters, has agreed to finalise this work by the end of 2013.

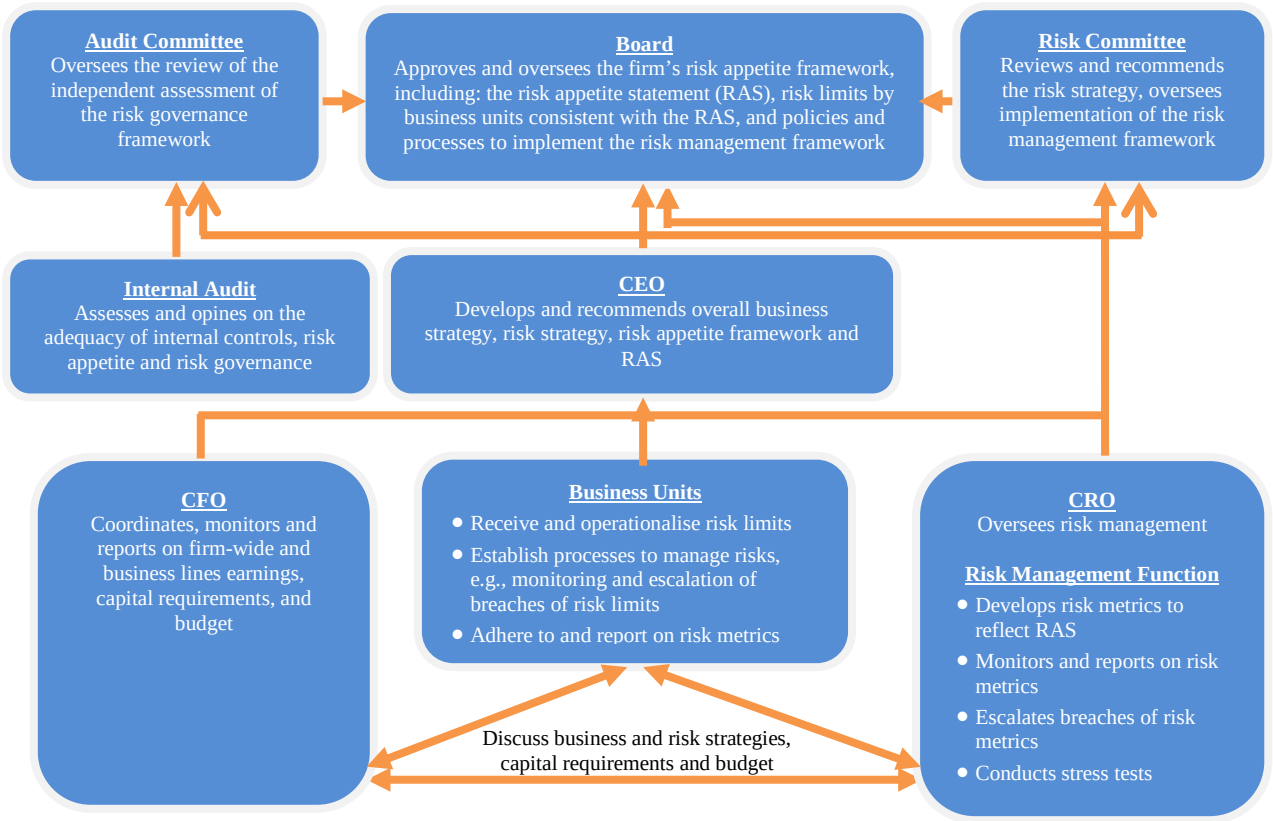
5. The FSB should consider launching a follow-up review on risk governance after 2016 (i.e., after the G-SIFI policy measures begin to be phased in), to assess national authorities' implementation of the recommendations to strengthen their supervisory guidance and oversight of risk governance. The review also should include the G-SIFIs identified in 2014 by the FSB in collaboration with the BCBS and IAIS.

I. Introduction

Increasing the intensity and effectiveness of supervision to reduce the moral hazard posed by SIFIs is a key component of the FSB's policy measures, endorsed by G20 Leaders.[7] Since the onset of the global crisis, supervisors have intensified their oversight of financial institutions, particularly SIFIs, so as to reduce the probability of their failure. Specifically, supervisory expectations of risk management functions and overall risk governance frameworks have increased, as this was an area that exhibited significant weaknesses in many financial institutions during the global financial crisis. While supervisors are responsible for assessing whether a firm's risk governance framework and processes are adequate, appropriate and effective for managing the firm's risk profile, the firm's management is responsible for identifying and managing the firm's risk.

In October 2011, the FSB agreed to conduct a thematic peer review on risk governance to assess progress toward enhancing practices at national authorities and firms (banks and broker-dealers).[8] For purposes of this review, risk governance collectively refers to the role and responsibilities of the board, the firm-wide CRO and risk management function, and the independent assessment of the risk governance framework (see Chart 2).

Chart 2: An example of a risk governance framework[9]



---

[7] See the 2010 FSB report on *Reducing the moral hazard posed by systemically important financial institutions*, which can be found at: http://www.financialstabilityboard.org/publications/r_101111a.pdf.

[8] See the 2011 FSB report on *Progress toward implementing the recommendations on enhanced supervision*, which can be found at: http://www.financialstabilityboard.org/publications/r_121031ab.pdf.

[9] The chart provides one example of a risk governance framework and does not advocate a specific risk governance framework or board structure.

- *Board responsibilities and practices*: The board is responsible for ensuring that the firm has an appropriate risk governance framework given the firm's business model, complexity and size which is embedded into the firm's risk culture. How boards assume such responsibilities varies across jurisdictions.
- *Firm-wide risk management function*: The CRO and risk management function are responsible for the firm's risk management across the entire organisation, ensuring that the firm's risk profile remains within the risk appetite statement (RAS) as approved by the board. The risk management function is responsible for identifying, measuring, monitoring, and recommending strategies to control or mitigate risks, and reporting on risk exposures on an aggregated and disaggregated basis.
- *Independent assessment of the risk governance framework*: The independent assessment of the firm's risk governance framework plays a crucial role in the ongoing maintenance of a firm's internal controls, risk management and risk governance. It helps a firm accomplish its objectives by bringing a disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. This may involve internal parties, such as internal audit, or external resources such as third-party reviewers (e.g., audit firms, consultants).

The peer review did not focus on other relevant dimensions of risk governance, such as risk disclosures and firm-wide compensation practices (since these areas have been covered by previous FSB peer reviews) or risk data aggregation capabilities at banks (since this topic is being covered by a task force of the BCBS. Separately, the International Association of Insurance Supervisors (IAIS) launched a peer review at the end of 2012 against its Core Principles on governance and risk management and internal controls.

There is currently no single set of principles and standards that comprehensively addresses and integrates risk governance requirements; however, a number of different standards and recommendations on good governance frameworks are relevant.[10] The review therefore did not assess compliance with any specific standard, but used a compilation of existing standards and recommendations (as appropriate) to take stock of risk governance practices at both national authorities and firms, and to identify any gaps therein. Supervisors were asked to evaluate firms' progress and the review team developed high-level criteria to provide some consistency to this exercise (see Annex A).

The findings of the review were based on the responses to questionnaires from FSB member jurisdictions[11] and from the 36 banks and broker-dealers that FSB members deemed as significant for the purpose of the review.[12] Annex B lists the firms surveyed.

---

[10] See *Risk Management Lessons from the Global Banking Crisis of 2008* by the Senior Supervisors Group (October 2009); *A review of corporate governance in UK banks and other financial industry entities – Final recommendations* (Walker Review, UK Treasury, November 2009); *Corporate Governance and the Financial Crisis – Conclusions and emerging good practices to enhance implementation of the Principles* by the OECD (February 2010); *Bank Governance: Lessons from the Financial Crisis* by Ard and Berg (World Bank Crisis Response Note 13, March 2010); *Corporate Governance in Financial Institutions: Lessons to be drawn from the current financial crisis, best practices* by the European Commission (June 2010); and *Toward Effective Governance of Financial Institutions* by the Group of Thirty (2012).

[11] The questionnaire completed by FSB national authorities can be found at: http://www.financialstabilityboard.org/publications/r_120404.pdf. The questionnaire for firms was very similar to that completed by national authorities but geared toward firms.

[12] In many jurisdictions, banking activities include broker-dealer functions which are addressed within the context of consolidated supervision. As such, the reference to firms throughout the report generally refers to banks.

Section II takes stock of national authorities' initiatives to strengthen oversight of firms' risk governance frameworks and describes the range of supervisory practices in four broad areas: (1) the board and its committees; (2) the firm-wide risk management function, including the CRO; (3) the independent assessment of the firm-wide risk management framework by internal audit and/or third parties; and (4) the supervisory assessment of risk governance frameworks.

Section III examines risk governance practices at surveyed firms and the changes made since the financial crisis. In addition to the responses to the questionnaire, the findings draw on the outcomes of discussions with industry organisations as well as risk committee directors and CROs of several firms that participated in the review. National supervisors were asked to assess firms' progress toward enhancing key risk governance functions, as well as the accuracy and completeness of the responses provided by firms headquartered in their jurisdiction.

Section IV sets out the conclusions and recommendations drawn from the findings of the review, which is followed by a list of sound risk governance practices (see Section V) that encompass an overlay of supervisory expectations for sound practices at firms.

II. National authorities' oversight of risk governance practices

Since the financial crisis, national authorities have increased their supervisory focus on risk governance, which is a critical element for promoting a more resilient financial system. Underpinning the range of reforms is the issuance in 2010 of the BCBS *Principles for Enhancing Corporate Governance* and the OECD publication on *Corporate Governance and the Financial Crisis – Conclusions and Emerging Good Practices.*[13] Some of the notable changes embedded in regulatory and supervisory guidance include:

- introducing explicit requirements for the establishment of a risk committee;
- conveying expectations to strengthen the risk management function, including the stature and qualifications of the CRO;
- introducing additional requirements for risk governance at SIFIs;
- enhancing the mandate and resources of supervisory authorities in relation to risk governance oversight;
- increasing the intensity of engagement between the supervisor and the board and senior management on risk governance issues; and
- adjusting the supervisory risk assessment process, particularly increasing the focus on risk governance across different business models.

Annex C provides more details on the initiatives FSB members have taken to strengthen oversight of risk governance practices, including implementation of other relevant principles such as the FSB principles for sound compensation practices[14] and recommendations put forward in the 2009 report by the Senior Supervisor Group (SSG) on risk management

[13] The 2010 BCBS paper can be found at http://www.bis.org/publ/bcbs176.pdf and the OECD paper can be found at: http://www.oecd.org/daf/corporateaffairs/corporategovernanceprinciples/44679170.pdf.

[14] The 2009 FSB *Principles for Sound Compensation Practices* can be found at: http://www.financialstabilityboard.org/publications/r_0904b.pdf.

practices during the financial crisis.[15] While supervisory guidance has improved, progress has been uneven across the functions that collectively form the risk governance framework. Based on the findings from the review, some areas where more supervisory requirements and/or guidance would be useful include:

- a clear definition of independence which is separate from non-executive director;
- the establishment of a stand-alone risk committee that is composed of independent directors;
- the level and types of risk information firms should provide as well as the frequency of risk reporting;
- the key features of an effective risk appetite framework to help supervisory evaluations; and
- the ways internal audit can provide feedback on whether a firm's risk governance processes are keeping pace with trends and/or align with best practices.

The next four sub-sections summarise existing supervisory expectations for the three key risk governance functions and examine authorities' approaches to assessing the implementation of supervisory expectations.

1. The board and its committees

Regulatory and supervisory guidance specifying the role and responsibilities of the board are prevalent across the FSB membership, including among other things for risk governance. A key responsibility of the board is to approve the firm's overall business strategy and RAF. As such, the board has ultimate responsibility for the firm's risk management, including setting the risk culture of the firm and overseeing management's implementation of the agreed business strategy. To ensure that boards are focused on the higher-level strategic and risk issues, supervisors are engaging more frequently with the board in particular with independent directors. The definition of what constitutes effective risk governance is evolving, however, supervisors highlight the importance of the board setting the "tone at the top" in regard to the firm's strategy and risk culture and challenging management on the adherence to the agreed risk appetite.

1.1 Board composition

The leadership structure to oversee the firm's risk management varies across jurisdictions. Most jurisdictions[16] require the establishment of a permanent audit committee, which has a longer history than other board sub-committees, driven by requirements from securities regulators to provide assurance to the quality of the financial information provided by registered financial institutions. As such, more specific regulatory and supervisory requirements for the composition and independence of the audit committee are set out than

[15] The 2009 SSG report *Observations on Risk Management Practices During the Recent Market Turmoil* can be found at: http://www.newyorkfed.org/newsevents/news/banking/2008/SSG_Risk_Mgt_doc_final.pdf.

[16] Argentina, Australia, Brazil (based on proportionality), Canada, China, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Saudi Arabia, Singapore, South Africa, Spain (for listed companies), Switzerland, Turkey, United Kingdom (based on proportionality), and United States.

for the risk committee. For example, a number of jurisdictions[17] require the audit committee to comprise a majority of independent or non-executive directors, several jurisdictions[18] require the audit committee chair to be independent (or in some cases a non-executive), and in a few jurisdictions the participation of the chair of the board is restricted.

The establishment of a stand-alone risk committee is less prevalent and the requirement typically applies to large, complex financial institutions (e.g., firms with many legal entities and/or cross-border operations). Where stand-alone risk committees exist, several jurisdictions[19] require risk committee members to have expertise in risk-related disciplines and only a few jurisdictions require a minimum number of independent directors. In Hong Kong, however, forthcoming changes will require all, or the majority, of the members of the risk committee to be non-executive directors.

Annex D provides further details on the regulatory and supervisory guidance for the composition of the board and sub-committees, but some of the key features include:

- *Independence:* Many jurisdictions[20] have established general requirements concerning the independence[21] of the board to ensure that there is objective judgement and decision-making on the board. Many jurisdictions[22] also set out quantitative minimums for the number of independent directors on the board. Some other jurisdictions only set quantitative minimums for the number of non-executive directors which does not necessarily ensure independent judgement on the board.
- *Expertise:* Regardless of the board structure, the board needs to comprise members who collectively bring a balance of expertise, skills, experience and perspectives while exhibiting the objectivity to ensure decisions are based on sound judgement and thoughtful deliberations. Many jurisdictions[23] conduct periodic reviews of the performance, training and skills needed in the board and risk committee. Requiring specific skills for all directors are a common practice (usually subsumed in "fit and proper" tests) and typically include relevant knowledge, experience and skills in finance and/or business. Several jurisdictions[24] not only look at individual qualifications but also take a holistic view of the board, examining their collective skills and qualifications. In addition to having certain skills and qualifications, some

---

17 Argentina, Australia, Canada, Hong Kong, Indonesia, Italy, Japan, Singapore, Turkey, and United States.

18 Australia, Hong Kong, India, Indonesia, Singapore, and South Africa.

19 Canada, France, Hong Kong, India, Indonesia, Japan, Singapore, and United States.

20 Australia, Canada, China, Hong Kong, India, Indonesia, Japan, Korea, Mexico, Saudi Arabia, Singapore, South Africa, Turkey, United Kingdom (defined only for non-executives), and United States.

21 The key characteristic of independence is the ability to exercise objective, independent judgment after fair consideration of all relevant information and views without undue influence from executives, controlling shareholders, or other external or third parties. Examples of relationships that could impair independence include a business relationship between the director and the firm (e.g., as vendor, audit partner, law partner) or a director who is a substantial shareholder of the firm. Some jurisdictions have a formal definition of independence that goes beyond that of a non-executive.

22 Canada, China, Germany (two-tier board system), Hong Kong, India, Indonesia, Italy, Korea (outside directors), Mexico, Netherlands, Singapore, South Africa, Switzerland, and United Kingdom (non-executive directors).

23 Argentina, Australia, Canada, China, Hong Kong, India, Indonesia, Italy, Japan, Netherlands, Saudi Arabia, Singapore, South Africa, Switzerland, Turkey, and United Kingdom.

24 Australia, Canada, China, Hong Kong, Italy, Netherlands, Singapore, and Switzerland.

jurisdictions[25] require directors to have the capacity to dedicate sufficient time and energy in reviewing information and developing an understanding of the key issues related to the firm's activities.

1.2 Governance of the board

For the board to effectively supervise and manage the firm's adherence to the agreed business strategy and risk appetite, directors should be provided and have access to comprehensive information about the firm's risks. This involves ensuring there are communication and reporting procedures across board sub-committees, and several national authorities set out such requirements in their guidance (see Annex E).[26] However, there is little supervisory guidance provided on the level and types of risk information firms should provide as well as the frequency of risk reporting. Importantly, the risk management reports provided to the board should contribute to sound risk management and decision-making. The board and its committees, however, should not just rely on the information management reports provided. They should consider if there is a need for additional risk-related information which should be made available to them when needed. Only a few jurisdictions[27], however, require the board to have such access.

2. The firm-wide risk management function

Since the financial crisis, national authorities have intensified their oversight of firms' risk management practices and raised their expectations for what is considered strong risk management, which is integral to the core business of a financial institution. The failure to have a strong, independent risk management function can lead to ill-informed boards and senior management teams as well as imprudent decisions. The risk management function should be responsible for the firm's risk management framework across the entire organisation, ensuring that the firm's risk limits are consistent with the RAS and that risk-taking remains within those limits. Stress tests and scenario analyses are viewed as a useful tool for identifying firms' vulnerabilities and developing risk management strategies to address the risks identified. To fulfil these responsibilities, risk management functions should be led by an influential and highly effective CRO.

2.1 Governance of the risk management function

Supervisors have increased their expectations for the risk management function and are evaluating the CRO's stature, authority, qualifications, and independence within the firm. As the crisis demonstrated, these are prerequisites for the CRO to be able to influence the firm's risk-taking activities directly and through the risk management function, and to effectively inform the board as risks evolve, are identified, and are taken. Annex F provides more information on the governance around the risk management function, but some supervisory practices regarding the CRO function include:

---

[25] Hong Kong, Italy, Singapore, and United States.

[26] Canada, China, Hong Kong, India, Indonesia, Italy, Japan, Mexico, Netherlands, Saudi Arabia, Singapore, Switzerland, and United Kingdom.

[27] Canada, Indonesia, Japan, and Singapore.

- *Independence*: Most jurisdictions[28] require the CRO and/or risk management function to be independent; that is, to have a distinct role from the other executive functions, revenue-generating functions and business line responsibilities.
- *Stature*: The CRO and risk management function should have sufficient stature in the organisation to influence the firm's risk-taking activities. In this regard, some jurisdictions[29] have supervisory guidance that requires the CRO to report and have direct access to the board. To elevate the CRO's stature, Singapore expects the dismissal of the CRO to be approved by the board.
- *Authority*: To effectively fulfil its role, many jurisdictions[30] require the CRO to have the authority to influence decisions that affect the firm's exposure to risk, and several jurisdictions[31] set out explicit expectations for the CRO to be able to challenge management's recommendations and decisions and communicate directly with senior management and with the board.
- *Qualifications*: "Fit and proper" tests are commonly used to assess the qualifications and competencies of the CRO in many FSB member jurisdictions.[32] In addition, the appointment of the CRO is approved by authorities in China, Germany (if the CRO is a member of the management board), and Singapore, while the United Kingdom interviews CRO candidates. Many jurisdictions[33] evaluate the CRO through their on-going supervisory processes.

2.2 Risk appetite framework

Assessing a firm's RAF is a challenging task that requires greater clarity and an elevated level of consistency among national authorities. At the core of the RAF is the firm's RAS, which has become an effective tool for enhancing the discussions between supervisors and boards about the firm's strategic direction in terms of risk taking. However, a key challenge toward assessing the effectiveness of a firm's RAS is a lack of common terminology for risk appetite, risk profile, and risk capacity used within firms, across firms and across national authorities.

This is an area that is developing in many jurisdictions; for instance, India, Russia and Saudi Arabia have looked at risk appetite only in context of the BCBS ICAAP, while in Canada, France and the United States, separate processes are continuing to be put in place to assess

---

[28] Argentina, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Turkey, United Kingdom (based on proportionality), and United States (for large banks).

[29] Australia, Canada, France, Germany, Hong Kong, Japan, Netherlands, Singapore, South Africa, and United States (for large banks).

[30] Canada, China, France, Germany, Hong Kong, India, Indonesia, Japan, Netherlands, Saudi Arabia, Singapore, South Africa, Turkey, United Kingdom, and United States (for large banks).

[31] Canada, France, Germany, Hong Kong, Korea, Singapore, and United States.

[32] Australia, China, Hong Kong, India, Indonesia, Japan, Korea, Netherlands, Saudi Arabia, Singapore, South Africa, Switzerland, Turkey, United Kingdom, and United States.

[33] Argentina, Brazil, Canada, France, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Singapore, South Africa, Switzerland, and United States.

firms' RAFs, often drawing on assessment criteria outlined in the work of the SSG.[34] Supervisory reviews are underway in Canada of firms' integration of their RAF with the strategic, financial and capital planning processes and compensation practices. In Hong Kong, firms' risk appetite is reviewed from an integrated firm-wide perspective taking into account all risks (financial and non-financial). The supervisor determines whether the firm's RAS is comprehensive and includes the appropriate risk targets that are consistent with each other. The supervisor will also determine whether the RAS has a wide range of measures and actionable elements and whether robust procedures and controls are in place for the setting and monitoring of the agreed risk appetite. National authorities in Singapore assess annually firms' link between risk appetite, strategic objectives, capital planning and operational budget planning. Supervisors also review the firm's progress in the translation of risk appetite into limits and triggers by risk type, as well as their monitoring and reporting procedures. In Switzerland, supervisors regularly review the risk limit frameworks and there must be an established link between the limits and the strategy.

2.3 Stress testing

The objective of stress tests and scenario analyses is to assess the unanticipated losses that a firm may incur under certain stress scenarios and the impact that may have on its business plans, risk management strategies or capital plans. The use of stress tests in firms' risk governance and capital planning has increased in recent years with the results serving as an input into the firm's strategic decision-making. As firms are increasingly linking stress test results to risk appetite, ICAAP[35], contingency planning[36], and recovery and resolution plans[37], supervisory approaches to stress testing are evolving accordingly. In Canada, supervisors assess whether chosen scenarios are appropriate for the portfolio of the institution, including severe shocks and periods of severe and sustained downturns, and where relevant, an episode of market turbulence or a shock to market liquidity and whether the frequency and timing of stress testing is sufficient to support timely management action. Similarly, supervisors in Hong Kong assess the coverage of stress tests and the types of stress scenarios and parameters chosen in relation to the firm's risk tolerance, overall risk profile and business plan; appropriateness of assumptions; adequacy of policies and procedures; the adequacy of the firm's contingency planning for action to be taken should a particular stress scenario happen; the level of oversight exercised by the board and senior management on the stress-testing program and results generated; and the adequacy of the firm's internal review and audit of its stress-testing program. Indeed, supervisory attention now includes both the outcomes of stress tests and the effectiveness of the firms' stress testing processes. For instance, Singapore, Switzerland and United Kingdom have dedicated teams to review stress testing practices at firms, and China, Germany, and Hong Kong expect firms' internal audit functions to assess the effectiveness of risk management systems in general, including stress tests.

---

[34] See the 2010 report by the Senior Supervisor Group (SSG) *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure*.

[35] Australia, Canada, Hong Kong, India, Italy, Singapore, and United States.

[36] Argentina, Brazil, Canada, France, Hong Kong, Indonesia, Italy, and Singapore.

[37] Australia, Canada, Germany, Hong Kong, South Africa, Singapore, United Kingdom, and United States.

3. Independent assessment of firms' risk governance framework

Strong internal control systems are a key element of sound risk governance. The board is responsible for overseeing the implementation of an effective risk governance framework, and as such, should directly oversee the independent assessment process. An assessment that is independent from the business unit and the risk management control function can assist the board in judging whether the risk governance framework, internal controls and oversight processes are operating as intended. This may be performed by internal audit or by third parties such as audit firms or consultants. Regardless of the approach, it is critical that the assessment result in an overall opinion on the design and effectiveness of the risk governance framework and be performed by individuals with the skills needed to produce a reliable assessment. Currently, audit functions at only a few firms provide overall opinions regarding the risk governance framework.

3.1 Internal audit

Across the FSB membership, regulatory or supervisory expectations exist for internal audit. Annex G provides a comparison of key regulatory and supervisory expectations with the most notable elements, including:

- *Independence*: Nearly all jurisdictions[38] require firms to have a permanent internal audit function that is independent from business lines, support functions (e.g., treasury, legal), and risk management. Firms are also required to explicitly link the independence of internal audit to auditor compensation or career plans.[39] Regardless of the direct reporting lines, most jurisdictions expect internal audit to have unfettered access to the board when reporting internal audit results.
- *Stature:* Several jurisdictions[40] expect internal audit to report directly to the board, a committee thereof, or an independent director. The direct reporting relationship involves the responsible party determining the CAE's compensation, completing the CAE's annual performance evaluation, approving the CAE's budget, and/or otherwise ensuring the CAE is not unduly influenced by the CEO or other members of the management team. While the CAE may report to the CEO on day-to-day administrative matters, all substantive decisions regarding the CAE and internal audit function are made at the board level. In Singapore, Hong Kong, and Indonesia, the dismissal of the CAE requires the audit committee's approval.
- *Qualifications:* All FSB members have established requirements or expectations for the CAE and internal audit staff to have the skills necessary to effectively carry out their duties. Supervisory assessments generally consider the technical knowledge, experience, and character of individuals within the internal audit function.

---

[38] A permanent internal audit function is not required in Korea but is a supervisory expectation, and is a requirement in the United Kingdom based on the proportionality principle.

[39] Australia, Brazil, Canada, China, France, Germany, Hong Kong, Indonesia, Italy, Korea, Mexico, Netherlands, Saudi Arabia, Singapore, South Africa, Switzerland, and United Kingdom.

[40] Brazil, Canada, China, Germany, Hong Kong, Indonesia, Italy, Singapore, and United States.

- *Scope, coverage, and frequency:* Many jurisdictions[41] expect internal audit to assess and/or opine on risk management or risk governance processes, as well as internal controls. Expectations for the scope, coverage, and frequency of such assessments vary widely. However, almost all jurisdictions expect internal audit to assess the organisation and mandates of the risk management function(s) and the adequacy of systems and processes for assessing, controlling, responding to, and reporting the firm's risks. No jurisdiction indicated that it expects internal audit to periodically provide a firm-wide assessment of risk management or risk governance processes.
- *Risk appetite framework:* Many jurisdictions[42] expect internal audit to assess compliance with the board-approved risk appetite. In the United Kingdom, internal audit is expected to ensure that procedures are in place to report breaches in the firm's risk appetite to the board.
- *Benchmarking:* Most jurisdictions[43] indicate that internal audit should be aware of industry trends/best practices and that auditors should consider such knowledge when conducting their work. However, no jurisdiction had specific expectations for internal audit to opine on whether a firm's risk governance processes are keeping pace with trends and/or align with best practices.
- *Remediation process:* There is a wide range of expectations for internal audit to follow-up on remedial actions to address material deficiencies and several jurisdictions expect internal audit to report the results of its follow-up activities to the board. Nearly all jurisdictions indicated that they require some form of follow-up and reporting.
- *Chief audit executive:* All jurisdictions indicate that supervisors consider the CAE's performance when assessing the quality of internal audit. Such assessments may be performed off-site, within on-site inspections, and/or through regular meetings with the CAE and internal audit staff. In Saudi Arabia, the appointment of the CAE requires a "no objection" from the central bank, and in Indonesia, banks are required to report to bank supervisors the appointment and dismissal of their CAE.

3.2 Third parties

Employing third parties could help to enhance the quality of firms' independent assessments by providing an unbiased opinion of a firm's risk governance framework as many internal audit functions are staffed with individuals whose experience may be limited to the practices employed by one or two firms. In addition, third parties often have a broader understanding of leading industry practices, especially in highly technical areas.

---

[41] Australia, Canada, China, France, Germany, Hong Kong, India, Indonesia, Mexico, Singapore, South Africa, Turkey, and United States.

[42] Australia, China, France, Germany, Hong Kong, Italy, Netherlands, Saudi Arabia, Singapore, South Africa, Switzerland, Turkey, and United States.

[43] Australia, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Switzerland, Turkey, United Kingdom, and United States.

Most jurisdictions[44] allow the use of third parties to assess a firm's risk governance framework, and in China and the Netherlands, the external auditor also assesses the effectiveness of the internal audit function. Many jurisdictions appropriately stipulate through regulation or guidance that: (i) the use of a third party does not relinquish the board or management from ultimate responsibility for ensuring the reliability of the independent assessments, and (ii) large and complex firms should not become overly reliant on third parties to provide expertise that should be developed within the firm's internal audit function. France specifically requires that outsourcing arrangements be engaged and overseen by internal audit to ensure independence and that internal audit maintains accountability for the scope, coverage, and frequency of work.

Several jurisdictions, however, restrict the use of third parties. For instance, in Italy, internal audit work can be outsourced only by small credit institutions with limited operational complexity. Meanwhile, in South Africa the central bank must approve any outsourcing activity, and in Korea, the use of third parties to assess a firm's risk governance framework is not regulated.

4. Supervisory approaches toward assessing risk governance frameworks

Supervisors play a crucial role in assessing the adequacy of a firm's risk governance framework and the practices employed by a firm to independently assess its framework. Supervisory expectations for risk governance practices outlined above are generally set out within the legal framework through a combination of legislation, regulation and supervisory guidance; however, the approach varies considerably across jurisdictions. Australia and Canada complement their standards with written guidance provided to the industry to assist with the implementation of prudential requirements and adoption of good practices.

Supervisory approaches toward assessing implementation of regulatory or supervisory guidance encompass a variety of steps (e.g., on-site inspections, off-site reviews, horizontal reviews). Supervisory assessments generally occur at least once a year across the FSB membership, though in Argentina assessments take place every 18 months and the United Kingdom is moving from a bi-annual assessment toward a system of continuous supervision. Several jurisdictions[45] take a risk-based approach to on-site examinations, focusing on riskier institutions. In the United States, national authorities have on-site teams with expertise to assess the governance practices at the largest and most complex banks on a real time basis. In China, joint regulatory meetings are held on a regular basis between the firm's head office, its branches, and the regulatory authority where the branches are located. Meetings with directors and senior management provide another avenue for national authorities to assess firms' risk governance practices. Annex H provides more information on the approaches taken to assessing firms' risk management frameworks.

---

[44] Argentina, Australia, Brazil, Canada, China, France, Hong Kong, India, Indonesia, Italy, Japan, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, United Kingdom, and United States.

[45] Argentina, Australia, Brazil, Canada, Hong Kong, Indonesia, Mexico, and Saudi Arabia.

Supervisors receive a wide range of risk reports or information from firms on their risk management practices, including from external auditors or other third parties as well as supporting documentation requested during on-site inspections. Standardised financial and risk reporting are a common practice; however, the types of reports or information provided varies. For instance, in Argentina, new reporting requirements will request quantitative measures for risk governance and formal exposure limits for each of the significant risks and stress test information; in Hong Kong and elsewhere, regular prudential reporting data and ad hoc requests for peer group analysis are utilised, e.g., stress test capital analysis and horizontal credit reviews of common (problem) loan accounts; and in Canada and Singapore, supervisory teams work with risk specialists to identify trends that can trigger additional investigations or reviews.

National authorities have access to a broad set of supervisory tools to incentivise firms to remediate deficiencies within their risk governance framework, depending on the severity of the deficiency. These tools include moral suasion, capital surcharges, restrictions on certain business activities, imposing fines and penalties, and the ultimate penalty of withdrawing bank licences. While a large number of supervisory authorities can use a number of these tools, a few have limited supervisory powers to scale the sanction based on the severity of the infraction, raising concerns over their ability to effectively intervene early where necessary when risks start to surface. Moreover, even though some national authorities have the authority to impose fines, this is difficult to implement in practice, for instance, due to cumbersome processes or supervisors lacking the will to act.

III. Firms' risk governance practices

The financial crisis spurred fundamental changes in risk governance practices at financial institutions, and in many cases, surveyed firms are ahead of regulatory and supervisory guidance. In general, surveyed firms that were most affected by the crisis have made the greatest advancements, perhaps necessitated by a need to re-gain market confidence. Firms that were less troubled from the crisis, however, have increased the intensity of the measures that they had in place pre-crisis. Some of the most obvious changes include:

- Consolidating and raising the profile of the risk management function across banking groups through the establishment of a group CRO, increasing the stature and authority of the CRO and increasing the CRO's involvement in relevant internal committees.
- Changing the reporting lines of the risk management function so that the CRO now reports directly to the CEO while also having a direct link to the risk committee.
- Intensifying the oversight of risk issues at the board through creation of a stand-alone risk committee, supported by greater links with the risk management function and other risk-related board committees, particularly audit and compensation committees. Cross-membership of the audit committee and risk committee is now quite common, with some firms involving (or at least inviting) the chair of the board, even the full board, onto the risk committee. The time commitment of independent directors has increased considerably over the past several years.
- Upgrading the skills requirements of independent directors on the risk committee and expecting these members to commit more time to these endeavours. The

composition of boards has changed considerably with many non-executive directors now having financial industry experience; the dominance of members from industrial companies or major shareholders is much less than a decade ago.

- Changing the attitude toward the ownership of risk across the firm with the business line now being much more accountable for the risks created by their activities than previously.

In addition to changing the composition and improving the strength of the board, there have been major developments in how firms analyse risks and the associated tools utilised such as RAFs, stress tests and reverse stress testing. One of the key lessons from the crisis was that reputational risk was severely underestimated; hence, there is more focus on business conduct and the suitability of products, e.g., the type of products sold and who they are sold to. As the crisis showed, consumer products such as residential mortgage loans could become a source of financial instability.

The next four sub-sections summarise the findings from the surveyed firms regarding the three key risk governance functions and provide a summary of the supervisory evaluations of firms' progress.

1. The board and its committees

The board is responsible for ensuring that the firm has an appropriate risk governance framework that is commensurate with the firm's strategy, complexity and size. The board's role and responsibilities for risk governance are generally defined in the board's charter and include approval of the firm's strategy and overseeing its implementation, setting out the guidelines and policies for risk management, and ensuring the firm's internal controls are robust. The board is also responsible for formulating the mandate and responsibilities of its committees such as the risk and audit committees. For instance, audit committees should ensure business units have effective remediation plans to address any control weaknesses noted by internal audit. Some firms have developed a Corporate Governance Framework or Code where all rules regarding the roles, responsibilities and oversight functions of the board are assembled. Establishing an enterprise or firm-wide risk management framework can help to provide an overview of risk policy architecture and process.

Having a stand-alone risk committee is a common practice even though it is not required by all national authorities. Firms generally ensure that the risk committee, which is responsible for overseeing senior management's implementation of the risk strategy, covers all the risks faced at the firm-wide level, including financial risks as well as operational, compliance, legal and regulatory risks. Regular meetings are held with senior management and the CRO to discuss performance of the business unit and compliance with the RAS and risk limits. Material risks are presented and discussed on both an aggregate basis and by type of risk. A few firms, however, noted the challenge of aggregating risks due to the complexity of the organisation, underscoring the importance of risk committees addressing information challenges arising from the complexity of large firms.

An effective governance structure has measures to prevent concentration of power and responsibility, such as requiring a number of independent directors, representation of certain skills and qualifications on the board, and the board regularly evaluating its effectiveness. It

is common for boards to have independent directors; some firms establish minimum quantitative requirements, ranging from a minimum of one-third to three-quarters of the board. Most firms provide a definition of independence in the board's charter, which is embedded in the firm's governance framework. The risk committee often comprises only independent directors. There is a wide range of practice regarding the qualifications for members of the board and risk committee; one firm highlighted that the skills required by the board are evolving, in part reflecting the risks taken by the firm. Some firms perform a matrix analysis of the experience and expertise of each director to identify skills needed from incoming directors. There is also a wide range of practice involving limitations linked to board structure, including: (i) the preclusion of the chair of the board from being chair of either the risk or audit committee; (ii) the separation of the roles of the CEO and chair of the board; and (iii) limited tenure on a committee.

Periodic reviews of the performance of the board and risk committee are a common practice. Reviews are conducted by the board nomination or governance committees or by the entire board. In some cases, external parties may be employed. Such reviews may include an assessment of training and skills needed on the board. In some firms, the board considers the functioning of its overall committee structure, including the number and types of committees and the highest and best use of board members' expertise. They also evaluate the reporting by the committees to the full board.

The board and risk committee are able to receive information, both formally and informally, directly from the CRO or the risk management function. It is becoming a common practice for the CRO to report information directly to the board; the risk reports are usually standardised in terms of formality, frequency and content. Both the overall risk level of the firm and information for each risk type are included in the reporting template (e.g., a heat map of identified risk categories across regions, global business, and a report with the top and emerging risks faced by the firm). Some firms explicitly define and document the information that the board and risk committee shall receive, set the agenda at the beginning of the year, and circulate to members in advance of meetings the relevant material to support the agenda item. Some firms require internal audit, or a third party, to verify the accuracy, comprehensiveness and completeness of information provided to the board and risk committee. Other firms satisfy themselves through discussions with management or conduct self-assessments of the effectiveness of the information provided to the board.

2. The risk management function

Since the financial crisis, many firms have improved risk management. Some of the most obvious changes relate to the governance processes around the risk management function; there also have been major changes in how risks are analysed and communicated and the associated tools that are utilised.

2.1 Governance of the risk management function

Since the financial crisis, many firms have strengthened how their risk management functions are structured, resourced, compensated, who the function is accountable to as well as its overall mandate. In many ways, these changes are bringing the governance arrangements for

the risk management function up to the standard that has typically applied to the internal audit function for several years. Firms are therefore encouraged to at least consider the validity of any remaining differences in governance processes that surround the two functions.

One of the most common improvements made by firms over the past five years has been to consolidate and raise the profile of the risk management function through the establishment of a group-wide CRO. The CRO and the risk management function generally have been given more stature, authority and independence compared to the pre-crisis period. Almost all firms reported that they now have a CRO with firm-wide responsibility for risk management who operates independently. Assessment of the CRO's stature, authority and independence includes the process for appointment, dismissal and performance evaluation of the CRO as well as the staffing requirements of the risk management function more generally. Only a few firms noted that the chair of the risk committee is involved in the performance assessment of the CRO. Further, only a few firms link the adequacy and qualifications of the risk management staff to an annual process that takes into consideration the strategy of the firm going forward.

Most firms noted that the CRO has a direct reporting line to the CEO (versus another business unit) which represents a major improvement since the crisis. However, there are still examples cited at a small number of firms where the CRO does not have a direct reporting line to the CEO. A few firms require the CRO to have a direct reporting line to the board, which helps to boost the stature of the CRO. A large number of firms also noted that their CRO is able to "access" the board, generally through the risk committee, but it is unclear how this is done in practice.

Almost all firms operate with a CRO who is separate from revenue-generating responsibilities or other executive functions (that is, "dual-hatting" of the CRO's responsibilities is avoided). Such a structure is essential for the CRO's independence. This separation of responsibilities has been reinforced by many firms re-structuring their risk management functions under a group-wide CRO, with regional or business line CROs having a direct reporting line to the group CRO, rather than to the regional or business line heads as had occurred in the past. To preserve the independence intended from such structures, 'dual-hatting' of responsibilities should also be avoided for those senior positions in the risk management function that report to the group CRO, particularly at globally active, complex firms. At some firms, the CRO reports to the CFO or, in a few exceptional cases, one person assumes the responsibilities of both the CRO and CFO. In addition, there are instances at some firms where the CRO is assigned other functional, albeit non-revenue generating, responsibilities. Where this relates to the oversight of functions such as compliance and anti-money laundering, the concern is more about the risk of over-burdening the CRO, particularly in more complex, global institutions, than the potential for conflict of interest per se.

Indeed, much progress has been made toward elevating the stature and independence of the CRO. While the role of the CRO has broadened and includes involvement in a number of key processes and internal committees that require inputs from the risk management function, other important processes warrant greater participation of the CRO, such as:

- *Mergers and acquisitions*. While the analysis of a proposed merger or acquisition would be submitted to the board or a committee for approval, the CRO generally takes part in the process as a member of the committee. Only a few firms require the CRO to prepare a formal risk opinion on planned mergers and acquisitions.
- *Strategic planning process.* Traditionally, the CRO is responsible for the oversight of the existing risk profile of the firm and of those risks being taken on a day-to-day basis as a result of previous business decisions. However, as indicated above, the CRO should also become increasingly involved, in a more proactive manner, in the activities and plans that deal with prospective business risk, including those risks which may arise from the execution of the firm's strategic business plan. The CRO should be involved in this process, from a risk perspective, by interacting with senior management and the board, understanding strategic business plans, and formally opining on the prospective risk profile and whether or not the firm has the necessary resources and systems to accommodate the resulting exposures. If such resources are not available, then space in the strategic plan should be created to ensure proper risk controls.
- *Treasury function*. Some firms have clearly defined the roles and responsibilities of the CRO regarding oversight of a firm's treasury function. However, there is a range of practice surrounding the organisational relationship between these two functions: (i) the independent liquidity risk control function has responsibility for the management and control of liquidity risk and that function reports directly to the CRO; (ii) the CRO participates as a voting member of the relevant management committee (typically the asset and liability management committee), with no specific role for the CRO defined; or (iii) the CFO alone is responsible for the treasury function without any oversight from the CRO in the risk management process.

2.2 Risk management tools

Two key additions to risk management tools have been (i) the development of RAFs and (ii) more robust and severe stress testing practices. Related to this, and given the under estimation of reputational risk pre-crisis, there now is much greater focus within many firms on business conduct and the suitability of products, e.g., the type of products sold and to whom they are sold.

The RAF is an increasingly important tool in centralising the focus on the firm's risk profile and providing a more integrated picture of the firm's risks. Firms indicated a good degree of understanding the key elements, objectives and uses of RAFs which are generally in line with recent studies such as the 2010 SSG report on developments in risk appetite frameworks and IT infrastructure.

Key features of a risk appetite framework (RAF)[46]

- RAFs help drive strategic decisions and right-size a firm's risk profile.
- RAFs establish an explicit, forward-looking view of a firm's desired risk profile in a variety of scenarios and set out a process for achieving that risk profile.
- RAFs include a risk appetite statement that establishes boundaries for the desired business focus and articulate the board's desired approach to a variety of businesses, risk areas, and in some cases, product types.
- The more developed RAFs are flexible and responsive to environmental changes; however, risk appetite is definitive and consistent enough to contain strategic drift.
- RAFs set expectations for business line strategy reviews and facilitate regular discussions about how to manage unexpected economic or market events in particular geographies or products.

Discussions with firms, however, reveal that there is significant variation in the perception of how much firms have progressed in the development, comprehensiveness and implementation of their RAFs. One of the key challenges is different interpretations of essential elements, including risk appetite, risk limits, and risk capacity.

- Some firms were able to report significant progress and have had an RAF for several years (in some cases since before the crisis). These firms' RAFs were linked to the firm's strategy and integrated with most other relevant internal processes such as budgeting, compensation plans, mergers and acquisition evaluations, new product approval, and stress testing. These firms were able to report that the understanding of the RAF was widespread both across functional lines and within multiple layers of their firm. They were also able to identify clear examples of how they had used their RAF in strategic decision-making processes, such as decisions to actively reduce the complexity of their operations. That said, even at these firms, it was recognised that operationalising an effective RAF is a continual journey that needs to evolve with changes in internal processes and the external environment.
- A number of firms reported that their implementation of an RAF was more recent and while it had been linked to the firm's strategy and integrated with some of the key internal processes, further work is envisaged, such as: linking the RAF with all the relevant internal processes; ensuring that qualitative as well as quantitative metrics are appropriately included; and somewhat relatedly, broadening the RAF to cover those harder to quantify risks, such as operational, compliance and reputation risks.
- For other firms, their RAFs are at an early stage of development. While they may have a high-level framework in place, numerous gaps exist. For example, the coverage may not extend to all relevant subsidiaries in the framework because the risk appetite is not clearly articulated at the business level nor integrated with all the relevant internal processes. Further, some RAFs are less developed in terms of including all the material risks the firm faces, particularly reputational and operational risks.

[46] Senior Supervisor Group (SSG) 2010 *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure*.

All firms surveyed considered risk limits to be the vehicle for operationalising the RAF at the business line level. The communication and escalation process for any breaches seemed to be very similar across the firms surveyed: the risk management function was responsible for monitoring risk limits, metrics, and breaches, and escalating any concerns; business units have to explain breaches to the risk management committee or board depending on the nature and size of the exposure; the authorisation of exceptions was defined top-down; and action plans were required. However, there were differences between firms in their approaches to departures from the RAF: some firms grant flexibility for a business line to depart from the RAF if the global risk appetite was not breached, whereas others give no flexibility for individual business lines to deviate from their business line risk limits.

Embedding the firm's agreed RAS into the firm's risk culture remains a challenge but several approaches have been taken by firms. A number of firms have developed training programs and manuals (with one firm requiring relevant employees to certify every year that they have attended the training program and read the manual), but only a few firms reported that they have linked core risk objectives to staff performance management processes. Discussions with firms revealed that a key to creating incentives for a better risk culture in firms is to link risk objectives with either compensation or career advancement prospects.

Stress testing has become a common tool for firms. The governance around group-wide stress testing typically involves firms developing their own historical and hypothetical scenarios, though national authorities can also set scenarios. The CRO and risk management function generally have a central role, acting as the owner of the process or participating in the committee leading the effort. The testing is conducted at least annually, and in many cases on a quarterly basis. Stress tests results are usually presented to the risk committee and sometimes to the national supervisor. These processes appear to be furthest developed in AEs, and some also perform reverse stress testing and counterparty stress testing. In contrast, some firms in EMDEs have not performed stress testing on an integrated basis or are still in the process of implementing their stress testing processes. Most firms use the stress testing results for their budgeting, RAF and ICAAP processes and to set contingency plans against stressed conditions.

3. Independent assessment of firms' risk governance framework

3.1 Internal audit

Firms primarily rely on their internal audit functions to independently assess their risk governance frameworks. In almost all cases, internal audit assesses the framework through a series of individual assurance audits, combined with some project-specific and other ongoing audit work. A few internal audit functions demonstrate the better practice of providing an overall opinion of the risk governance framework on an annual basis. In line with expectations established by national authorities, all of the firms' internal audit functions are organisationally separate from business lines and have unfettered access to the board.

Almost every firm reported that they have made changes to strengthen their internal audit functions since 2008. Major changes include: appointing a CAE; establishing more attractive compensation plans and career paths for internal auditors; increasing both the number and skills of internal audit staff; expanding internal audit's role/responsibilities, including

participating as an observer at risk management committees and decision-making processes; and enhancing business monitoring.

Internal audit's role and responsibilities are primarily established via an audit charter, with audit manuals detailing procedures for planning, executing, and reporting audit's work. At all surveyed firms, internal audit is responsible for assessing risk management or risk governance processes as well as internal controls. While national authorities' expectations vary, most internal audit functions also assess:

- the appropriateness of assumptions used in scenario analysis and stress testing,
- the degree to which the firm's risk governance is keeping pace with industry trends and aligns with best practices,
- the quality and adequacy of resources within the risk management function,
- the overall efficiency and integrity of risk management information systems, and
- the effectiveness of the risk and issue escalation process.

Most firms indicated that internal audit plays a role in monitoring whether the business and risk management units are operating according to the RAF. However, some firms rely primarily on the independent risk management function for this assessment. Internal audit's role is generally to test that practices align with the processes and procedures established in the RAF, though a few firms expect internal audit to also opine on the appropriateness of the limits and other tolerances established in the RAF. Given that many RAFs are in the early stages of evolution, some firms noted that internal audit's role and responsibilities related to the RAF are still being defined and implemented.

Firms reported a wide range of practices with regard to the format and content of reporting to the board. At several firms, the CAE provides regular reports to the board or audit committee, summarising the results of internal audit's work, including overall conclusions or ratings, key findings, material risks/issues, and follow-up of management's resolution of identified issues. Meanwhile, some internal audit functions only provide the board or audit committee with a periodic synthesis of internal audit activity or a "report on audit reports", which does not seem sufficient to ensure the board can carry out its responsibilities within the risk governance framework.

3.2 Third parties

Approximately half of the firms that participated in the peer review indicated that they have used third parties to assess their firm's risk governance framework or components of the framework. The rest of the firms indicated that they used third parties to provide perspectives and benchmarks related to regulatory expectations and industry best practices associated with risk governance frameworks, or significant aspects of those frameworks, with this information being used to promote upgrades in firm practices. Such an approach was seen as helpful in meeting the continual challenge of developing and maintaining risk governance frameworks that keep abreast of changing legislative/regulatory environments along with an evolving economic and competitive landscape.

3.3 Escalation processes

All firms reported having internal policies, procedures, and/or processes to facilitate employees reporting concerns and issues within the firm. These are in addition to external complaint and whistle-blower processes established by supervisors. Some firms described having processes tailored to different types of issues (e.g., issues impacting financial results and related disclosures versus general issues related to risk and/or control breakdowns).

- For sensitive information, most firms have established an internal "whistle-blowing" hotline and offer employees anonymity and other protections from negative consequences to the extent possible under the relevant laws of the jurisdiction.
- For non-sensitive information, processes generally involve employees reporting to a direct supervisor or senior manager within the business unit and/or to an individual within an independent risk, compliance, and/or audit function or legal department.

3.4 Evaluation of the effectiveness of the independent assessment

While there is no common practice for comprehensively evaluating the effectiveness of the independent assessment of the risk governance framework, most firms have several processes in place for assessing the work of the internal audit function. Some of the key processes and/or criteria used include:

- the number of internal audits that cover risk management topics during the course of an audit cycle,
- the number and types of risk management issues identified by internal audit,
- results of internal audit's quality assurance activities,
- results of periodic internal audit self-assessments and/or assessments performed by external parties,
- quality of information provided to the audit committee, and
- compliance with the Institute of Internal Auditors' (IIA) professional standards.

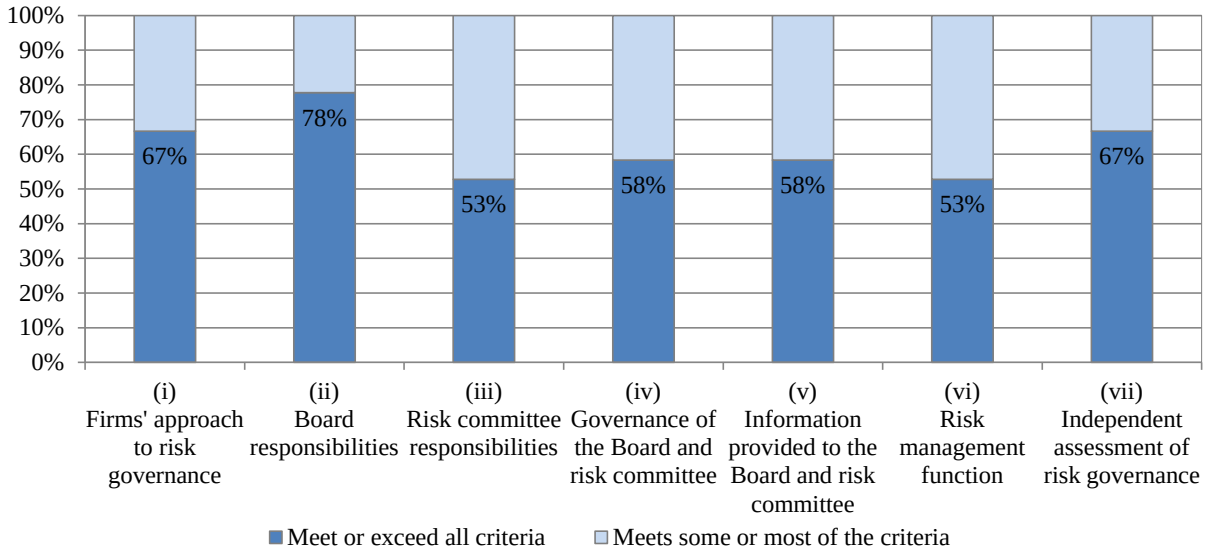
4. Supervisory evaluations of risk governance practices

The peer review asked supervisors of surveyed firms to evaluate firms' progress toward enhanced risk governance across seven broad areas. To help provide some consistency to this exercise, high-level evaluation criteria were developed (see Annex A) and the supervisory evaluations were reviewed for all surveyed firms; G-SIFIs; and by region. The criteria were developed by drawing from a compilation of relevant principles, recommendations and supervisory guidance, and are considered by the review team as the fundamental preconditions for effective risk governance frameworks.

In summary, surveyed firms have made the most progress in strengthening (ii) the role and responsibilities of the board, with nearly 80 per cent of surveyed firms evaluated by national supervisors as meeting or exceeding all of the criteria (see Chart 3 below). This is an area that warranted significant changes but is also viewed as comparatively easy to implement. More work, however, is needed by supervisors to assess the true effectiveness of the board's oversight of the firm. Further, despite significant improvements in (i) firms' approaches to risk governance and (vii) the independent assessment of the risk management function,

significant gaps remain. Roughly 50 per cent of surveyed firms failed to meet all of the criteria in (iii) having defined responsibilities of the risk committee and (vi) the risk management function. These areas need much greater attention on the part of both supervisors and firms.

Chart 3: Supervisory evaluations for all surveyed firms

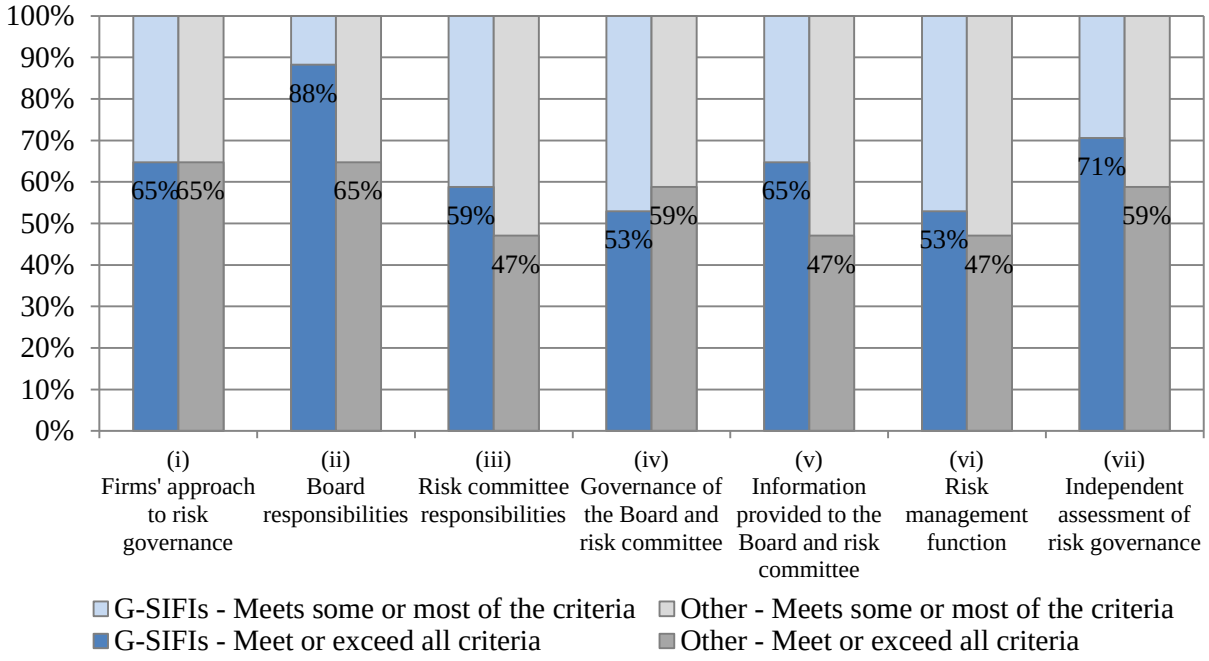


The supervisory evaluations indicate that, among the G-SIFIs surveyed, more progress has been made toward enhancing risk governance practices relative to other surveyed firms, particularly in (ii) board responsibilities, (iii) risk committee responsibilities; (v) information provided to the board and risk committee, and (vii) the independent assessment of risk governance (see Chart 4 below). While G-SIFIs are also more advanced in (vi) the risk management function, this area is one of the weakest at surveyed G-SIFIs across the seven risk governance areas evaluated. One of the key hindrances to effective risk management at G-SIFIs has been weaknesses in firms' IT infrastructures and the inability to aggregate risk data efficiently. While progress is being made, some supervisors noted their firm could not complete the FSB Data Gaps common data template for G-SIFIs. This common data template aims to address key information gaps identified during the crisis and provide a strong framework for assessing potential systemic risks.[47] However, G-SIFIs identified in November 2011 and November 2012 are expected to meet higher expectations for risk data aggregation capabilities and risk reporting beginning in January 2016.[48]

[47] See the FSB *Data Gaps Initiative – A Common Data Template for Global Systemically Important Banks* which can be found at: http://www.financialstabilityboard.org/publications/r_120328l.pdf.

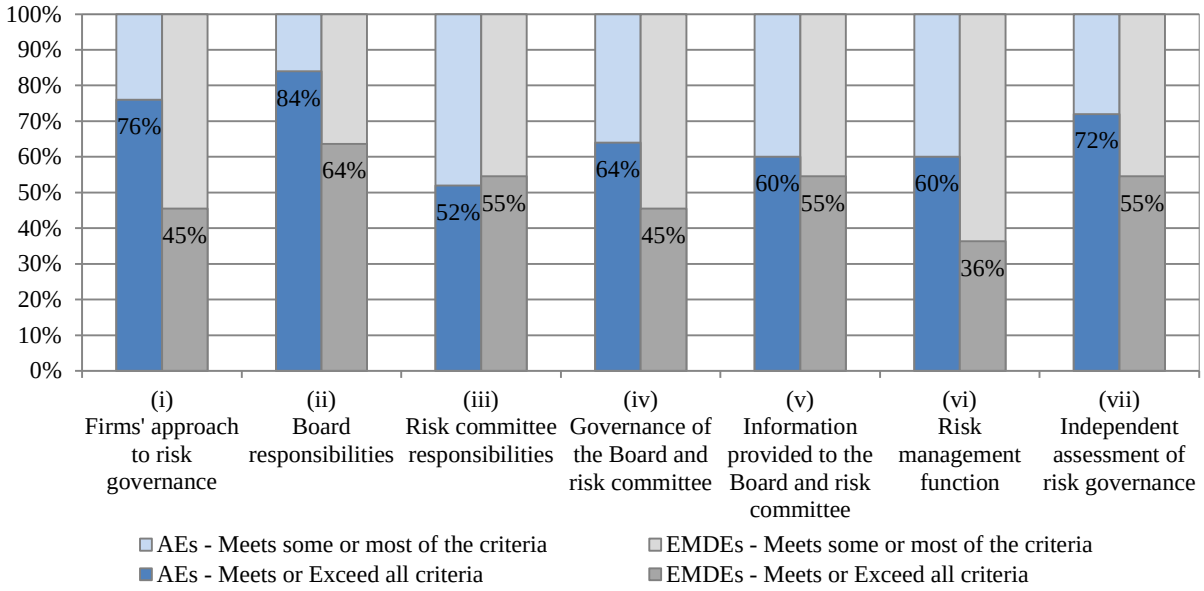
[48] See the BCBS *Principles for effective risk data aggregation and risk reporting* which can be found at: http://www.bis.org/publ/bcbs239.pdf.

Chart 4: Supervisory evaluations by type of institution



By region, firms that reside in AEs have generally progressed further than those in EMDEs across all aspects of the areas evaluated, except for (iii) risk committee responsibilities (see Chart 5 below). This aligns with the finding that firms that were hardest hit during the financial crisis have made the most progress as such firms largely reside in advanced economies. These firms experienced a significant turnover in senior management and directors, including more non-executive directors, but board oversight of risk through an established risk committee is weak across regions. For EMDEs, risk governance practices need to be significantly enhanced; in particular in the (vi) risk management function as approximately 65 per cent of surveyed firms do not meet all of the criteria. Other areas where more work is needed is in their (i) approach to risk governance and (iv) governance of the board and risk committee where more than 50 per cent of firms do not meet all of the evaluation criteria. These gaps need immediate attention.

Chart 5: Supervisory evaluations by region



IV. Conclusions and recommendations

Much progress has been made toward enhancing risk governance frameworks at surveyed firms since the crisis. Nonetheless, this progress has been uneven across the functions that collectively form the risk governance framework – the board, the firm-wide risk management function, and the independent assessment of risk governance. Specifically, firms have made most progress in defining the role and responsibilities of the board, but much more needs to be done to strengthen the role of the risk committee and the CRO and risk management function. Continued weaknesses in risk management will undermine the effectiveness of the changes made to board oversight of the firm's risk governance framework. To ensure that progress continues toward achieving more effective risk governance frameworks, a more integrated and consistent approach across all aspects of the risk governance framework has to be developed. Such an approach will require a shift in attitude for both firms and supervisors as this requires taking a holistic view of all aspects of the risk governance framework rather than looking at each facet in isolation.

Drawing from the survey responses and discussions with risk committee directors and CROs, this report sets out a list of sound risk governance practices that should help supervisors to enhance their oversight of risk governance at financial institutions, in particular at SIFIs (see Section V). While none of the surveyed authorities and firms exhibited all of these sound practices, many firms' practices tended to be more advanced than the guidance provided by national authorities.

Recommendation 1: To ensure that firms' risk governance practices continue to improve, FSB member jurisdictions should strengthen their regulatory and supervisory guidance for financial institutions, in particular for SIFIs, and devote adequate resources (both in skills and quantity) to assess the effectiveness of risk governance frameworks. In particular, national authorities should take into consideration the set of sound risk governance practices identified during the peer review.

Recommendation 2*:* The relevant standard setting bodies (e.g., BCBS, IAIS, IOSCO, OECD) should review their principles, taking into consideration the sound practices for risk governance listed in Section V.

Recommendation 3: Risk culture plays a critical role in ensuring effective risk governance endures through changing environments. The FSB Supervisory Intensity and Effectiveness group has agreed to implement the recommendation from the 2012 FSB progress report on enhanced supervision to explore ways to formally assess risk culture, particularly at G-SIFIs. This work should be completed by September 2013.

As the supervisory evaluations revealed, both national authorities and firms need to focus on strengthening firms' risk management functions. Effective risk governance is based on a well-designed and articulated firm-wide risk management framework, which reflects the firm's risk culture, enumerates the firm's risk profile, and ensures that the risk limits set out in the agreed RAS are not breached. The risk limits have to be properly defined and calibrated and align with compensation as well as escalation processes that enable appropriate action to be taken if the firm is operating outside its risk appetite and risk limits. Developing an effective RAF, however, remains a challenge for most firms; firms need to make further

progress in linking their RAFs to business strategies so that RAFs become truly effective and operational tools.

Recommendation 4: To improve their ability to assess firms' progress toward more effective risk management, national authorities should provide guidance on the key elements that are incorporated in effective risk appetite frameworks. To enable firms to define frameworks with a minimum amount of comparability despite their firm-specific nature, a common nomenclature for terms used in risk appetite statements (e.g., "risk appetite", "risk capacity", "risk limits") should be established. The FSB Supervisory Intensity and Effectiveness group, in collaboration with relevant standard setters, has agreed to finalise this work by the end of 2013.

Effective internal control systems are a key element of sound risk governance, and supervisory expectations for the independent assessment of internal control systems by internal audit were well established prior to the crisis. This includes guidance issued by the BCBS as early as 1998[49] and by a longer history of regulatory requirements for publicly-traded financial institutions, including permanent audit committees and independent CAEs. Since the crisis, many supervisors have appropriately elevated their expectations of internal audit functions to include more qualitative assessments of policies, procedures, risk limits and risk exposures. As such, this is an area that demonstrated relatively sound practices across the FSB membership for both national authorities and financial institutions. Nearly all firms have an independent CAE who reports administratively to the CEO or audit committee chair and who directly reports audit findings to a permanent audit committee. Despite the wide range of sound practices, there is still room for improving the CAE's access to directors beyond those on the audit committee. Regulators also need to elevate and convey expectations for internal audit, and/or a third party, to periodically provide a firm-wide assessment of risk management or risk governance processes.

Finally, to promote further progress toward effective risk governance, the report recommends that another peer review be conducted.

Recommendation 5: The FSB should consider launching a follow-up review on risk governance after 2016 (i.e., after the G-SIFI policy measures begin to be phased in), to assess national authorities' implementation of the recommendations to strengthen their supervisory guidance and oversight of risk governance. The review also should include the G-SIFIs identified in 2014 by the FSB in collaboration with the BCBS and IAIS.

V. Sound risk governance practices

Drawing from the findings of the review, including discussions with industry organisations as well as risk committee directors and CROs of several firms that participated in the review, the

[49] The BCBS published a paper *Framework for internal control systems in banking organisations* in September 1998 which can be found at: http://www.bis.org/publ/bcbs40.pdf. In August 2001, the BCBS published a paper *Internal audit in banks and the supervisor's relationship with auditors.* This paper was superseded by principles on *The internal audit function in banks* published by the BCBS in June 2012, which can be found at http://www.bis.org/publ/bcbs223.pdf.

report sets out a list of sound risk governance practices. The list extracts some of the better practices exemplified by national authorities and firms. The sound practices also build on some of the principles and recommendations published by other organisations and standard setters, drawing together those that are relevant for risk governance. This integrated and coherent list of sound practices aims to help national authorities and firms continue to improve their risk governance.

The board of directors

1. The board:
    a) avoids conflicts of interest arising from the concentration of power at the board (e.g., by having separate persons as board chairman and CEO or having a lead independent director where the board chairman and CEO are the same person);
    b) comprises members who collectively bring a balance of expertise (e.g., risk management and financial industry expertise), skills, experience and perspectives;
    c) comprises largely independent directors and there is a clear definition of independence that distinguishes between independent directors and non-executive directors;
    d) sets out clear terms of references for itself and its sub-committees (including tenure limits for committee members and the chairs), and establishes a regular and transparent communication mechanism to ensure continuous and robust dialogue and information sharing between the board and its sub-committees;
    e) conducts periodic reviews of performance of the board and its sub-committees (by the board nomination or governance committee, the board themselves, or an external party). This includes reviewing, at a minimum annually, the qualifications of directors and their collective skills (including financial and risk expertise), their time commitment and capacity to review information and understand the firm's business model, and the specialised training required to identify desired skills for the board or for director recruitment or renewal;
    f) sets the tone from the top, and seeks to effectively inculcate an appropriate risk culture throughout the firm;
    g) is responsible for overseeing management's effective implementation of a firm-wide risk management framework and policies within the firm;
    h) approves the risk appetite framework and ensures it is directly linked to the business strategy, capital plan, financial plan and compensation;
    i) has access to any information requested and receives information from its committees at least quarterly;
    j) meets with national authorities, at least quarterly, either individually or as a group.

2. The risk committee:
    a) is required to be a stand-alone committee, distinct from the audit committee;
    b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;
    c) includes members who are independent;
    d) includes members who have experience with regard to risk management issues and practices;
    e) discusses all risk strategies on both an aggregated basis and by type of risk;
    f) is required to review and approve the firm's risk policies at least annually;
    g) oversees that management has in place processes to ensure the firm's adherence to the approved risk policies.
3. The audit committee:
    a) is required to be a stand-alone committee, distinct from the risk committee;
    b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;
    c) includes members who are independent;
    d) includes members who have experience with regard to audit practices and financial literacy at a financial institution;
    e) reviews the audits of internal controls over the risk governance framework established by management to confirm that they operate as intended;
    f) reviews the third party opinion of the design and effectiveness of the overall risk governance framework on an annual basis.

The risk management function

4. The CRO
    a) has the organisational stature, skill set, authority, and character needed to oversee and monitor the firm's risk management and related processes and to ensure that key management and board constituents are apprised of the firm's risk profile and relevant risk issues on a timely and regular basis. The CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities as well as a direct reporting line to the board and/or risk committee;
    b) meets periodically with the board and risk committee without executive directors or management present;
    c) is appointed and dismissed with input or approval from the risk committee or the board and such appointments and dismissals are disclosed publicly;
    d) is independent of business lines and has the appropriate stature in the firm as his/her performance, compensation and budget is reviewed and approved by the risk committee;

e) is responsible for ensuring that the risk management function is adequately resourced, taking into account the complexity and risks of the firm as well as its RAF and strategic business plans;

f) is actively involved in key decision-making processes from a risk perspective (e.g., the review of the business strategy / strategic planning, new product approvals, stress testing, recovery and resolution planning, mergers and acquisitions, funding and liquidity management planning) and can challenge management's decisions and recommendations;

g) is involved in the setting of risk-related performance indicators for business units;

h) meets, at a minimum quarterly, with the firm's supervisor to discuss the scope and coverage of the work of the risk management function.

5. The risk management function:

a) is independent of business lines (i.e., is not involved in revenue generation) and reports to the CRO;

b) has authority to influence decisions that affect the firm's risk exposures;

c) is responsible for establishing and periodically reviewing the enterprise risk governance framework which incorporates the risk appetite framework (RAF), risk appetite statement (RAS) and risk limits.

i. The RAF incorporates an RAS that is forward-looking as well as information on the types of risks that the firm is willing or not willing to undertake and under what circumstances. It contains an outline of the roles and responsibilities of the parties involved, the risk limits established to ensure that the framework is adhered to, and the escalation process where breaches occur.

ii. The RAS is linked to the firm's strategic, capital, and financial plans and includes both qualitative and quantitative measures that can be aggregated and disaggregated such as measures of loss or negative events (e.g., earnings, capital, liquidity) that the board and senior management are willing to accept in normal and stressed scenarios.

iii. Risk limits are linked to the firm's RAS and allocated by risk types, business units, business lines or product level. Risk limits are used by management to control the risk profile and linked to compensation programmes and assessment.

d) has access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis; risk-bearing affiliates and subsidiaries are captured by the firm-wide risk management system and are a part of the overall risk governance framework;

e) provides risk information to the board and senior management that is accurate and reliable and periodically reviewed by a third party (internal audit) to ensure completeness and integrity;

f) conducts stress tests (including reverse stress tests) periodically and by demand. Stress test programs and results (group-wide stress tests, risk categories and stress test metrics) are adequately reviewed and updated to the board or risk committee. Where stress limits are breached or unexpected losses are incurred, proposed management actions are discussed at the board or risk committee. Results of stress tests are incorporated in the review of budgets, RAF and ICAAP processes, and in the establishment of contingency plans against stressed conditions.

Independent assessment of the risk governance framework

6. The board requires a periodic independent assessment of the firm's overall risk governance framework and provides direct oversight to the process.

7. The board or audit committee fully support the CAE and internal audit function by ensuring the CAE:

   a) is organisationally independent from business lines and support functions and has unfettered access to the audit committee;

   b) meets regularly with audit committee members outside of management's presence;

   c) is appointed and dismissed with the approval of the audit committee (or chair of that committee);

   d) has his/her performance, compensation, and budget reviewed and approved by the audit committee;

   e) has the organisational stature, talent, and character needed to provide a reliable independent assessment of the firm's risk governance framework and internal controls and not be unduly influenced by the CEO and other members of management;

   f) has the resources (people and systems) needed to effectively carry out the responsibilities of internal audit;

   g) provides regular reports to the board or audit committee which summarise the results of internal audit's work, including overall conclusions or ratings, key findings, material risk/issues, and follow-up of management's resolution or identified issues.

8. The audit committee and risk committee periodically meet to ensure effective exchange of information, to ensure effective coverage of all risks include emerging risk issues relative to the RAF and business plans.

9. Internal audit meets its obligations to the board and supervisors by:

   a) reporting audit findings, significant issues, and the status of remedial action directly to the board or audit committee on a regular basis;

   b) providing an overall opinion of the design and effectiveness of the risk governance framework to the audit committee on an annual basis;

c) providing qualitative assessments of risks and controls as opposed to evaluating compliance with policies and procedures;

d) assessing whether business and risk management units are operating according to the RAF;

e) providing feedback on how the firm's risk governance framework and RAF compare to industry guidance and better practices as a means of influencing their evolution;

f) providing input to risk assessments and feedback on internal controls during the design and implementation processes;

g) escalating issues and concerns identified in the course of audit work or through internal whistle-blowing, complaint, or other processes and situations where appropriate remedial action is not being implemented in a timely manner;

h) being aware of industry trends and best practices;

i) meets, at least quarterly, with the supervisor.

10. Third parties

a) supplement (but do not replace) internal audit staff to increase coverage;

b) complement internal audit's skill sets with deeper expertise in select areas and/or broader context of industry practices;

c) are effectively supervised by the board or internal audit function to ensure accountability remains within the firm.

Annex A: Supervisory evaluation criteria

Template for national authorities to evaluate firms' risk governance practices

1. Firm's approach toward risk governance *Based on the firm's responses to questions 1.1 to 1.4*	
Criteria	• The firm has made some fundamental changes in how it approaches risk governance and is able to identify three key fundamental changes made. • The firm has evaluated whether the risk governance framework aligns with international standards or best practices, such as the BCBS principles for enhancing corporate governance, the recommendations set out in the SSG risk management lessons from the global financial crisis of 2008. • The firm has a blueprint in place for developing its strategic plan. • The firm has a process for reviewing the strategic plan on a regular basis and does so in practice. • The firm has a process in place to evaluate whether it is operating within its strategic plan. • The firm has an *effective* process for communicating the strategic plan throughout the firm. • The CRO or equivalent is actively involved in the development of the strategic plan for the firm. • The roles of the CRO, CFO and Treasurer in the development of the strategic plan are appropriately and clearly differentiated. • For firms whose structure includes wholly-owned bank/broker-dealer subsidiaries, the strategic plan is formulated and applied at the group level. • The firm has developed an overall risk appetite framework (RAF) and the RAF is linked to the firm's strategy, capital plans, funding plans and budget. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*****:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

2. Board responsibilities and practices **A. Defined roles and responsibilities for the board** *Based on the firm's responses to questions 2.1*	
Criteria	• The firm has a *sufficient* definition and documentation concerning the role and responsibilities of the board for risk governance: • The board approves the firm's strategic plan (e.g., risk tolerance, risk appetite, business strategy). • The board oversees senior management's implementation of the firm's strategic plan. • The board approves and oversees the implementation of the firm's policies for risk, risk management and compliance relating to risk management. • The board approves and oversees the implementation of the firm's internal controls system relating to risk management. • The board formulates and defines the mandate and responsibilities of board-level committees dealing with risk governance. • The roles and responsibilities of the board are *explicitly and adequately* adapted to the firm's size, business model, complexity and systemic importance. • The firm's responses show that the role and responsibilities of the board are practically implemented *in an appropriate and effective manner*. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*****:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

2. Board responsibilities and practices B. Defined roles and responsibilities for the risk committee *Based on the firm's responses to questions 2.2*	
Criteria	• The firm explicitly defines and documents the role and responsibilities of the risk committee. • The risk committee is a self-standing committee. • The risk committee advises the board on the firm's overall current and future risk tolerance/appetite and strategy. • The risk committee ensures the strategic plans covered by the risk committee include those for capital and liquidity management, as well as for credit, market, operational, compliance, reputational and other risks of the firm; there are few risks that are not included in the strategic plan. • The risk committee oversees senior management's implementation of the strategic plans. • The mandate of the risk committee takes into account the group structure in which the firm operates. • The risk committee discusses the firms' material risks on both an aggregated basis and along the types of risks borne by firms (e.g., credit risk, market, liquidity, operational risks). • The roles and responsibilities of the risk committee are *explicitly and adequately* adapted to the firm's size, business model, complexity and systemic importance. • The firm's responses show that the role and responsibilities of the risk committee are practically implemented *in an appropriate and effective manner*. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*****:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

2. Board responsibilities and practices **C. Governance of the board and risk committee** *Based on the firm's response to question 2.3*	
Criteria	• The firm has an *adequate* framework for defining, documenting and monitoring the governance of the board's and risk committee's practices. • The firm has a sufficient definition and documentation concerning the composition of the board and risk committee, including a minimum proportion of independent members and a clear definition of independent member. • The firm clearly defines and documents the qualifications for members of the board and risk committee, including passing fit and proper tests and possessing certain skills (e.g., technical financial understanding in risk disciplines, business experience in risk issues). • The firm limits the chair of the board's involvement/participation in the risk committees (e.g., the chair of the risk committee cannot be the chair of the board). • The firm has an established process for reporting from the risk committee to the board and from the board to the risk committee. • The firm has an established process for the co-ordination and communication among different board sub-committees that deal with issues relevant for overall risk assessments. • The firm periodically reviews the performance, training and skills needed in the board and risk committee. • The firm periodically reviews the functioning of the overall committee structure used by the board. • The firm's responses show that the governance of the board's and risk committee's practices is explicitly and adequately adapted to the firm's size, business model, complexity and systemic importance. • The firm's responses show that a periodic review of the functioning of the governance of the board's and risk committee's is practically conducted in an appropriate and effective manner. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*****:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

2. Board responsibilities and practices D. Information provided to the board and risk committee *Based on the firm's responses to question 2.4*	
Criteria	• The firm explicitly defines and documents the information the board and risk committee shall receive, or be able to request, from the firm (e.g., CRO, risk management function, internal audit) and third parties (e.g., external auditors, consultants, other experts). • The board/risk committee is able to receive information, both formally and informally, directly from either the CRO or the risk management function. • The firm's responses show that the information channel between the board/risk committee and the CRO or the risk management function is practically functioning in *an appropriate and effective manner*. • The information received by the board/risk committee is standardised in terms of form, frequency and content. • The board/risk committee receives detailed information for each type of risk and each business unit, not just for the overall firm. • The board and risk committee have metrics or a process to satisfy themselves that the risk reports and information they receive are accurate, comprehensive, and depicts an appropriate view of your firm's risk profile. • An independent model validation unit exists and reports to the risk committee and other relevant bodies. • The board/risk committee has access to external expert advice. • The firm's responses show that the level of information provided to the board/risk committee is *explicitly and adequately* adapted to the firm's size, business model, complexity and systemic importance. • The firm's responses show that the routines for reporting from the risk committee to the board and from the board to the risk committee are practically implemented in *an appropriate and effective manner*. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*****:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

3. Risk management function *Based on the firm's responses to questions 3.1 to 3.14*	
Background	The independent risk management function is responsible for the firm's risk management framework across the entire organisation, ensuring that the firm's risk meets the desired risk profile as approved by the board. The risk management function is responsible for identifying, measuring, monitoring, recommending strategies to control or mitigate risks, and reporting on risk exposures.
Criteria	• Mandate of CRO / risk management includes responsibility for identifying, measuring, monitoring, assessing risks, and recommending actions to manage/mitigate risks, on an enterprise-wide basis. • The firm has an independent senior executive with enterprise-wide responsibility for risk management (e.g., CRO or equivalent). • The CRO or equivalent does not have any business line responsibilities, i.e., is not responsible for a profit centre and there is no dual hatting. • The firm's CRO reports to the CEO, and also reports and has direct access to the board and its risk committee without impediment. • The CRO meets with the chair of the risk committee on a regular basis. • The CRO meets with the risk committee without management present. • A process exists to assess the adequacy of risk management resources (in number and quality). Process includes: – A breakdown by risk type; – Comparisons to prior year; – Links to strategic initiative and objectives; – Information provided to the risk committee for approval; – Is a part of the firm's budgeting process; – Evaluation of information technology systems, system development resources. • Risks are identified and monitored on an ongoing basis, including both quantitative and qualitative elements. • Sufficient and comprehensive risk information is provided to the board/risk committee for decision-making purposes. • The firm utilises forward-looking stress tests and scenario analysis to understand potential risk exposures. Results are communicated to business lines and individuals. • The firm's new product approval process includes input by risk management relative to potential risks, linkages to the firm's risk appetite statement, etc. • If adequate risk management processes are not in place, new product offerings are delayed until systems and risk management are able to accommodate the relevant activity. • The firm's merger and acquisition process includes a proactive role for risk management relative to the identification of risks, impact on the overall risk profile of the firm, an assessment relative to the overall risk appetite statement, etc. • Risk management provides independent/objective reporting of risks to the board and senior management on a regular basis, and ad hoc where necessary/requested. • Risk reporting includes risk exposures, the results of stress tests or scenario analysis. • Risk monitoring and risk reporting are done on an aggregate and disaggregated basis. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm

3. Risk management function *Based on the firm's responses to questions 3.1 to 3.14*	
	has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

4. Independent assessment of risk governance framework *Based on the firm's responses to questions 4.1 to 4.12*	
Criteria	• The firm has an internal audit function and requires that function to undertake, on a regular basis, an independent assessment (e.g., independent from the business unit and risk management function) of the firm's risk governance framework and risk management policies and processes at the enterprise level, legal entity level, and/or for selected revenue-generating business units. • The internal audit function reports directly to the board or a board-level committee, such as the audit committee, from an organizational perspective and with regards to findings. • Where relevant, the hiring of third parties (e.g., consultants, external auditors) to conduct the assessment of the firm's risk governance framework and risk management policies and processes are independent from the business unit or activities for which it is conducting its reviews. • The firm's board and senior management review internal audit reports, prudential reports, and/or external expert reports as part of the firm's risk governance framework. • The firm has made changes to strengthen how internal audit operates since 2007. • The firm has a process for evaluating and ensuring that the head of internal audit and internal audit personnel have appropriate qualifications. • The firm has processes in place to facilitate the communication of significant (or specific) concerns/situations/behaviours by individuals within your firm to the board, senior management, and national authorities (e.g., escalation process and/or whistle-blowing). • The firm's board and senior management monitor the timely remediation of weaknesses identified through the independent assessment of the risk governance framework and underlying functions. • The firm has a process to evaluate the effectiveness of the independent assessment of its risk governance framework. • The firm has demonstrated that it doesn't over-rely on external third parties instead of growing resources internally when resources will be required on a permanent basis. • For firms whose structure includes a separate bank/broker-dealer operating as a wholly-owned subsidiary, the same requirements/processes described above are applied consistently throughout the group. ***Exceeds criteria***: The firm's range of practices meets all of the criteria and the firm has an effective means of monitoring their effectiveness. ***Meets all criteria:*** The firm's range of practices meets all of the criteria and the firm has plans to make additional changes. ***Meets majority of the criteria:*** The firm's range of practices meet the majority of the criteria and the firm has plans to make additional changes. ***Meets some of the criteria*:** The firm's range of practices meet a few of the criteria and the firm does not have plans to make any further changes.

Annex B: Surveyed firms

FSB Member Jurisdiction	Financial institution*
Argentina**	1. Banco Galicia
Australia	2. Commonwealth Bank of Australia
Brazil**	3. Banco Itaú
Canada	4. Royal Bank of Canada
China**	5. Bank of China* 6. Industrial and Commercial Bank of China
France	7. Credit Agricole* 8. Societe Generale*
Germany	9. Deutsche Bank* 10. Helaba
Hong Kong	11. HSBC (local subsidiary of HSBC)
India**	12. HDFC Bank
Indonesia**	13. Bank Mandiri
Italy	14. Unicredit Group* 15. Intesa San Paolo Group
Japan	16. Mitsubishi UFJ FG* 17. Mizuho FG* 18. Sumitomo Mitsui FG*
Korea	19. Kookmin Bank
Mexico**	20. Banamex (local subsidiary of Citibank)
Netherlands	21. ING Bank* 22. Rabobank
Russia**	23. Sberbank of Russia
Saudi Arabia**	24. The National Commercial Bank
Singapore	25. DBS Bank
South Africa**	26. FirstRand Limited
Spain	27. Santander* 28. BBVA*
Switzerland	29. Credit Suisse* 30. UBS*
Turkey**	31. Turkiye Garanti Bankasi
United Kingdom	32. HSBC* 33. Lloyds Banking Group
United States	34. Citigroup* 35. Goldman Sachs* 36. Wells Fargo*
Total	**36 (of which 17 are parent G-SIFIs)**

* Financial institutions identified as G-SIFIs in November 2012.
** Emerging markets and developing economies (EMDEs).

Annex C: Key changes in oversight of risk governance

	Self-assessed national guidance against international principles				Initiatives to strengthen oversight of risk governance practices
	BCBS[50]	OECD[51]	FSB[52]	SSG[53]	
Argentina	✓	✓			• Issued domestic guidelines on corporate governance and risk management. • Adjusted Supervision Manual to be in line with the guidelines.
Australia	✓		✓		• Reviewed corporate governance practices for continued effectiveness. • Introduced new governance requirements linking remuneration to risk practices.
Brazil	✓	✓	✓		• Issued regulation on application of corrective measures. • Increased use of intrusive, conclusive supervision. • Increased interaction between supervisors and the board, its sub-committees and management. • Increased focus on business models and link between business and risks.
Canada	✓	✓	✓	✓	• Strengthened capabilities by establishing in 2010 a dedicated Corporate Governance Division responsible for the assessment of corporate and risk governance practices. • Currently updating Corporate Governance Guideline (initially issued in 2003).
China	✓		✓		• Enhanced macro-prudential regulation. • Implemented Basel III, increased requirements on capital and liquidity, established regulation on leverage ratios and loan loss provisioning. • Enhanced risk management practice through guiding financial institutions to conduct stress tests. • Strengthened supervision of SIFIs and set the policy measures to reduce risks of SIFIs.
France	✓	✓			• Strengthened regulation to incentivise banks to upgrade their practices in order to have a strong and clear risk management at the group and enterprise levels.
Germany	✓	✓	✓	✓	• Strengthened requirements for the risk management function, CRO skills and stature, and internal controls. • Changed risk rating process. • Increased focus on business models and link between business and risks.

[50] BCBS 2010 *Principles for effective corporate governance*, which can be found at: http://www.bis.org/publ/bcbs176.htm.

[51] OECD 2004 *Principles of corporate governance*, which can be found at: http://www.oecd.org/daf/corporateaffairs/oecdprinciplesofcorporategovernance.htm.

[52] FSB 2009 *Principles for sound compensation practices*, which can be found at: http://www.financialstabilityboard.org/publications/r_0904b.pdf.

[53] SSG 2009 *Risk management lessons from the global banking crisis of 2008*, which can be found at: http://www.sec.gov/news/press/2009/report102109.pdf.

Annex C: Key changes in oversight of risk governance

	Self-assessed national guidance against international principles				Initiatives to strengthen oversight of risk governance practices
	BCBS[50]	OECD[51]	FSB[52]	SSG[53]	
Hong Kong	✓	✓	✓	✓	• Enhanced supervisory guidelines related to risk governance oversight. • Changed risk rating process. • Increased interaction between supervisors and management.
India	✓	✓			• Enhanced supervisory guidelines to emphasis corporate governance and risk management. • Restructured to continuously and closely monitor financial conglomerates. • Reviewed the entire supervisory system to bring it in line with global best practices. • Changed risk rating process from CAMELS to risk-based supervision. • Strengthened supervisory skills through specialised training. • Increased frequency of interactions between supervisors and management. • Enhanced supervisory co-operation with host supervisors. • Inspecting overseas branches of Indian banks.
Indonesia	✓	✓	✓		• Changed risk rating process. • Require self-assessment. • Revised risk management regulation. • Revising GCG regulation to incorporate FSB principles for sound compensation practices and BCBS principles for enhancing corporate governance.
Italy	✓	✓	✓		• Increased interaction between supervisors and the board and risk committee. • Increased focus on fit and proper issues for the board and executives. • Increased focus on dynamics within the board and its oversight of management. • Require that the build-up of macro-prudential risks be taken into account.
Japan	✓	✓	✓	✓	• Increased the intensity of the regulatory regime and requirements for SIFIs. • Expanded reach of supervision. • Increased supervisory personnel and budget. • Implemented G20 recommendations.
Korea	✓				
Mexico	✓	✓	✓		• Implemented Basel III.

Annex C: Key changes in oversight of risk governance

	Self-assessed national guidance against international principles				Initiatives to strengthen oversight of risk governance practices
	BCBS[50]	OECD[51]	FSB[52]	SSG[53]	
Netherlands	✓	✓	✓		• Strengthened capabilities of supervisors in corporate and risk governance. • Increased the use of intrusive, conclusive supervision. • Increased focus on fit and proper issues for the board and executives. • Increased focus on dynamics within the board and its oversight of management. • Increased focus on culture, control environment, and codes of conduct.
Russia	✓	✓			• Issued new laws on consolidated supervision and risk management systems. • Expanded reach of supervision. • Moved responsibility for supervision.
Saudi Arabia	✓	✓	✓		• Implemented Corporate Governance Regulations. • Implemented Basel II; Basel II.5 and III are being implemented within the BCBS timeframe. • Strengthened review of banks' risk governance practices, which is a mandatory part of on-site inspection and other supervisory reviews.
Singapore	✓	✓	✓	✓	• Enhanced the Corporate Governance Regulations and Guidelines. • Increased focus on risk governance in supervisory engagements.
South Africa	✓	✓	✓		• Require a risk committee and/or more engagement of boards in risk management.
Spain	✓	✓			• Strengthened requirements around corporate governance structures. • Changed the risk rating process.

Annex C: Key changes in oversight of risk governance

	Self-assessed national guidance against international principles				Initiatives to strengthen oversight of risk governance practices
	BCBS[50]	OECD[51]	FSB[52]	SSG[53]	
Switzerland	✓	✓	✓		• Increased the intensity of the regulatory regime and requirements for SIFIs. • Upgraded capabilities of supervisor in corporate and risk governance as well as in remuneration supervision. • Increased interaction between supervisors and the board/Risk committee; on remuneration, direct interaction with the Remuneration Committee. • Increased focus on fit and proper issues for the board and executives. • Increased focus on dynamics within board and its oversight of management. • Increased focus on culture, control environment, codes of conduct. • Refined approach to risk analysis to calibrate frequency and intensity of supervision. • Increased focus on business models and link between business and risks, including cross-border risks. • Increased/more robust use of third parties in regulatory audits.
Turkey	✓			✓	• Changed risk rating process. • Amended guidelines on corporate governance. • Increased interaction between the supervisors and the board and/or risk committee.
United Kingdom	✓	✓			• Increased the intensity of the regulatory regime and requirements for SIFIs. • Moved focus to relationship management supervision.
United States	✓				• Increased the intensity of the regulatory regime and requirements for SIFIs. • Require a risk committee and/or more engagement of boards in risk management. • Expanded reach of supervision. • Moved responsibility for supervision. • Increased coordination among financial regulators. • Increased focus on dynamics within board and its oversight of management.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Argentina	• The number and composition required to facilitate an independent opinion. • At least 80% to have financial experience. • Suitability, professional qualities and performance in related areas.	• Yes, required based on size and economic importance. • Majority should be independent; those who are not must possess relevant knowledge and skills.	• Yes, required. • Minimum of 2 directors and person responsible for internal audit. • Majority of members to be independent. • Members are reviewed bi-annually.	
Australia	• Majority (and chair) to be independent. • Collectively, have the knowledge, skills, experience to understand the risks. • Annual fit and proper tests.	• Not required, but expected for major banks. • Arrangements for audit committee create clear expectation of desirable practice.	• Yes, required. • Chair of the board may sit on the audit committee, but cannot chair the committee. • All members are to be non-executive directors.	A non-executive director who is free from any business or other association – including those arising out of a substantial shareholding, involvement in past management or as a supplier, customer or adviser – that could materially interfere with the exercise of their independent judgment.
Brazil	• Not required, but participation of independent members is encouraged and assessed during supervision. • Adequate technical and unblemished background.	• Not required, but a general practice.	• Yes, required; based on proportionality principle. • At least 1 member must be recognized as an accounting and finance expert.	

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Canada	• Minimum of 7 directors, of which no more than ⅔ are to be affiliated with the bank. • Forthcoming guidance to address skills explicitly.	• Under forthcoming guidance: o Depending on the nature, size, complexity and risk profile, the board should establish a dedicated risk committee. o All members, including the chair, should be non-executives. o Reasonable representation of individuals with sufficient knowledge of risk management. o Where appropriate the committee should include individuals with technical knowledge of risk disciplines that are significant to the financial institution.	• Yes, required in legislation. • All members should be non-executives of the financial institution.	A director is 'affiliated' with a bank if, in the opinion of OSFI, the director has a significant or sufficient commercial, business or financial relationship with the bank or with an affiliate of the bank to the extent that the relationship can be construed as being material to the director and can reasonably be expected to affect the exercise of the director's best judgment.
China	• Independent members to have tertiary degree and over 5 years of experience. • More than 3 independent directors for banks with regulatory capital exceeding RMB 1 billion. • Fit and proper requirements.	• Yes, required. • Adequate knowledge and experience in relevant areas.	• Yes, required. • Chair is to be an independent director.	A director without any other position in the bank or relation with the bank and its shareholders that may affect his independent and objective judgment.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
France	• Not required.	• Not required. • If a standalone committee exists, to comprise only non-executive directors. • At least 1 member must have expertise in finance or accounting.	• Not required.	
Germany	• Independence ensured through 2-tier board structure. • Must have the expertise necessary to fulfil their control function. • Fit and proper requirements for both tiers of the board.	• Not required, but a practice among complex institutions • Chair of a stand-alone risk committee can only be from the supervisory board. • Can be established at the supervisory body as a self-standing committee, which means all members are independent, or its responsibilities can be shared among several committees.	• Not required, but a practice among complex institutions. • Chair of the stand-alone audit committee must be a member of the supervisory board. • Can be established at the supervisory body as a self-standing committee, which means all members are independent, or its responsibilities can be shared among several committees.	No precise definition, but BaFin/Bundesbank demand statements from members of the supervisory board concerning other business relationships with the institution that could have an impact on the independence of the member, as a well as a statement concerning family relationships.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Hong Kong	• At least ⅓ or 3 of the directors, whichever is higher, should be independent. • Collectively, has adequate knowledge and expertise relevant to each of the bank's material business activities and the associated risks. • Fit and proper requirements.	• Not required, but strongly encouraged. • All, or the majority, of the members to be non-executive directors and have risk discipline experience.	• Yes, required. • All members should be non-executive directors, the majority of whom, including the chairman, should be independent. The audit committee as a whole should have recent and adequate experience and should possess a collective balance of skills and expertise to discharge its responsibilities.	A non-executive director (i.e., not an employee of the firm and does not hold any other office in the institution in conjunction with his office as director) who is independent of management and free from any business or other relationship that could materially affect his independent judgment. Independence is the ability to exercise objective, independent judgment after fair consideration of all relevant information and views without undue influence from executives or from external parties.
India	• Not less than ½ to be non-executive directors. • If non-executive chair, then at least ⅓ to be independent; if an executive director, then at least ½ to be independent. • At least ½ the members should have experience or knowledge in a pre-defined set of areas. • Fit and proper requirements.	• Yes, required. • The chair is an expert in the area. • Members of the risk committee are independent of business decisions.	• Yes, required. • Chair is to be an independent director. • Minimum of 3 directors, of which ⅔ to be independent. • All members of the audit committee shall meet certain qualifications and at least one member shall have accounting or financial management expertise.	An independent director is a non-executive director. Apart from receiving director's remuneration, does not have any material pecuniary relationships or transactions with the company, its promoters, its senior management or its holding company, its subsidiaries and associated companies.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Indonesia	• Fit and proper requirements.	• Yes, required. • Risk management committee composed of independent board members (commissioners) and parties. • Risk monitoring committee composed of independent members (commissioners) and independent parties with expertise in finance and risk management.	• Yes, required. • audit committee composed of independent board members (commissioners) and independent parties with expertise in finance or accounting, and law or banking.	Does not have any relation regarding financial, management, ownership and/or family connections with other members of the board, management or controlling shareholder, which may affect his/her ability to act independently.
Italy	• Adequate number of non-executive members. • Number of independent member commensurate with the size of the board and business model. • Fit and proper requirements.	• In large and operationally complex companies is required an internal control committee, which is in charge of both risk control and audit. • The risk committee must include independent members.	• For large and operationally complex companies, an internal control committee is required which is in charge of both risk controls and audit. • The audit committee must include independent members.	Detailed rules concerning the definition of independence are to be issued by the Minister for the Economy and Finance pursuant to Article 26 of the Consolidated Law on Banking. In the meantime supervisors encourage banks to adopt a definition of independence, in their bylaws, so to assure that some directors are independent from the management and from relevant shareholders.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Japan	• Adequate experience and knowledge.	• Not required. • Adequate experience and knowledge of risk management.	• Yes, required. • Majority of committee members to be outside directors.	Is not a partner or an executive of the statutory audit firm or the internal audit firm that is associated with the company, and has not been a partner or an executive of any such firm for the last 3 years. This also applies to legal firm(s) and consulting firm(s) that have a material association with the entity.
Korea	• Outside directors to be 3 or more and over ½ of the board. • Experience and knowledge of finance.	• Not required. • Recommended that outside director chair the committee.	• Yes, required.	Is not a supplier, service provider or customer of the firm. This should also include lessor-lessee type relationships.
Mexico	• At least ¼ to be independent. • Experience and knowledge of finance and the law.	• Yes, required. • Comprise at least 2 directors, the CEO, the persons responsible for risk management and internal audit.	• Yes, required. • At least 1 independent director is required to reside on the audit committee. • All members are non-executive directors. • At least 1 director has to have experience in finance or audit and internal control.	Is not a substantial shareholder of the firm, i.e., owning 2% or more of the block of voting shares, does not work for the institution (among many other criteria).

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Netherlands	• Supervisory board to have at least 3 members; ½ to be independent. • Suitability based on knowledge, skills and conduct.	• Required for major banks. • No requirements for independent directors.	• Not required.	Independence criteria reflect the ability to act objectively, critically and independently.
Russia	• Executive directors could total maximum ¼ of the board. • A sufficient number are expected to be independent. • Relevant education and knowledge.	• Not required, but a common practice at major banks. Best practices have been brought to the attention of firms.	• Not required, but best practices have been brought to the attention of firms.	It is recommended that independent members should neither be an owner (shareholder), nor affiliated party to the firm or its auditor for the last 3 years.
Saudi Arabia	• A sufficient number are to be independent. • Fit and proper requirements.	• Not required, but encouraged and a common practice at major banks.	• Yes, required. • Members require accounting and finance skills.	Independence is infringed where: shareholding exceeds 5%; held a senior management within the group in the past 2 years; family relationship with another board member or senior executive within the group; a board member elsewhere in the group; held a senior management position with an affiliated company within the past 2 years (e.g., external auditor).

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Singapore	• Majority to be independent. • Chair to be a non-executive director. • Fit and proper requirements.	• Yes, required. • At least a majority (including the chair) to be non-executive directors and at least 2 directors with relevant technical skills in risk disciplines or business experience.	• Yes, required. • All non-executives and at least a majority (including the chair) to be independent and at least 2 directors with accounting or related financial management expertise of experience.	One who is independent from any management and business relationships with the bank, independent from any substantial shareholder of the bank and has not served on the board of the bank for a continuous period of 9 years or longer.
South Africa	• Not more than 49% to be employees. • Chair not to be an employee. • Fit and proper tests.	• Yes, required. • At least 3 directors, of which at least 2 are non-executive directors.	• Yes, required. • Chair of the board should not be a member of the audit committee.	Not being an employee of the bank or its subsidiaries or the controlling company or subsidiaries of the controlling company.
Spain	• An adequate share to be independent, executives and shareholders. • Education, experience, independence and dedication.	• Yes, required. • Adequate share to be non-executive members. • Education, experience, independence and dedication are assessed.	• Yes, required for listed firms. • Chair must be an independent director and at least 3 non-executive members.	
Switzerland	• All directors (including chair) are prohibited from serving management positions. • At least ⅓ to be independent. • Fit and proper requirements.	• Not required but expected and is a common practice at major banks. • The chair of the board should not be a member of the committee. • Majority of must be independent.	• Yes, required. • Majority of its member must be independent, and have accounting skills and experience with internal and external audit. • The chair of the board should not be a member of the audit committee.	Independence criteria include: • currently or within the last 2 years, held no other function at the firm; • currently or within the last 2 years was not the external lead auditor. • no business relations which could lead to conflicts of interest.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
Turkey	• An adequate proportion to be independent. • CEO and the chair of the board shall not be the same person. • Majority to have experience and knowledge of banking or business administration. • Fit and proper requirements.	• Not required, but the board may decide to transfer its duties regarding risk management to an officer or officers or a self-standing sub-committee. • The responsibility for risk management may only be assigned to one of the non-executive directors or to a committee composed of such directors or to the audit committee.	• Yes, required. • Minimum 2 members of the board. • Members shall be appointed among the non-executive directors of the board. • Members shall bear the qualifications set by the board.	Neither an owner (shareholder), affiliated party to the credit institution, have qualified shares in the bank or their partners subject to consolidation, have been partners or staff of audit firms of the banks or their partners subject to consolidation or providing rating, valuation or outsource services to them or they are not involved in the processes of independent audits, rating or valuation for the banks or their partners subject to consolidation, nor its auditor for the last 2 years; should possess the experience and education to make judgments independently of owners, executives and other board members.
United Kingdom	• Expect majority to be non-executive directors. • Expect chair of the board to be a non-executive director.	• Firms to consider establishing based on proportionality. • The chair should be a non-executive director. • Members should be predominantly non-executive directors.	• Yes, subject to proportionality. • Yes, it should have an appropriate number of non-executive directors.	Only non-executive director defined.

Annex D: Regulatory and supervisory guidance – Composition of the board and sub-committees

	Board composition and skill requirements	Risk committee 1. Self-standing committee required 2. Composition and skill requirements	Audit committee 1. Self-standing committee required 2. Composition and skill requirements	Definition of independent director (which differs from a non-executive director)
United States	• Knowledge of the banking industry and regulations and laws governing the firm.	• Not required but encouraged; changes underway to make a requirement. • Majority of a self-standing committee must be independent. • Forthcoming changes will require the number of independent directors to be based on the nature of operations, asset size and other criteria. At least 1 expert in risk management will be required.	• Yes, required. • Composed entirely of independent directors and include members with banking or related financial management expertise.	In general, a non-management director that is free from any family relationship or any material business or professional relationship (other than stock ownership and the directorship itself) with the firm or its management. For purposes of audit committee membership: • For publicly traded firms, the director does not accept any consulting, advisory, or other compensatory fee from the firm and cannot be an affiliated person of the firm or subsidiary of the firm. • For all insured depository institutions, the director is not, and within the preceding fiscal year has not been, an officer or employee of the firm or affiliate. • For insured depository institutions with assets greater than $3 billion, independence also means not a large customer of the firm.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
Argentina	• Not required.	• No required reporting to/from the risk committee to the board, but assessed during supervision. • No required reporting among sub-committees but a supervisory practice.	• Yes, information is required to be in a standard form and contain certain minimum information. • Guidelines exist for each type of risk. • The board has to be knowledgeable about governance of subsidiaries. • No reporting frequency is specified.	• Yes, annual reviews are required for both the performance and skills needed on the board and risk committee and the overall functions of the board's committee structure. • Set out in role of board.
Australia	• Required for the audit committee.	• No required reporting to/from the risk committee to the board, but prudent to do so. • No required reporting among sub-committees.	• No requirement for information to be in a standard form, but expect the board to set clear reporting protocols and to receive adequate information to assess risks. • The level of risk reporting detail is at discretion of board. • No reporting frequency is specified.	• Yes, fit and proper assessments are required annually. • No requirement for the board to review the functions of its committee structure, but expected and assessed during supervision.
Brazil	• Required for the audit committee and compensation committee.	• No required reporting to/from the risk committee to the board, but encouraged and assessed during supervision. • No required reporting among sub-committees but encouraged and assessed during supervision.	• Financial institutions are not required to appoint a CRO. • Yes, information is required to be in a standard form and contain certain minimum information. • Yes, required to show overall risk level and for each type of risk and each business unit. • Reporting frequency is at least annual.	• No requirement to review the performance and skills needed on the board (and risk committee) nor to review the functions of the board's committee structure, but expected and assessed during supervision.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
Canada	• Yes, required under board assessment criteria (2002).	• Yes, under board assessment criteria, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • No prescribed requirements for the types of risk information to be provided. • No reporting frequency is prescribed, but expect at a minimum quarterly for conglomerate banks. • Evaluated under board assessment criteria.	• Yes, under board assessment criteria, annual reviews are required for both the performance and skills needed on the board and risk committee and the overall functions of the board's committee structure. • Forthcoming guidance requires the board to have a skills evaluation process, incorporating such tools as a competency matrix, which should be reviewed annually and updated by the appropriate board committee. Directors should seek internal or external educations/training opportunities in order to fully understand the risks undertaken by the financial institution.
China	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • Yes, required to provide information on the overall risk level or information for each type of risk and each business unit. • No reporting frequency is specified.	• Yes, reviews are required for the performance and skills needed on the board and risk committee. • No requirement to review the overall functions of the board's committee structure, but assessed during supervision.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
France	• Not required.	• No required reporting to/from the risk committee to the board and among sub-committees, but expected and assessed during supervision.	• Yes, information is required to be in a standard form and contain certain minimum information. • Suitable summary statements are required; risk specifics are not detailed. • Reporting frequency is at least annual.	• No requirement to review the performance and skills needed on the board and risk committee nor to review the functions of the board's committee structure, but expected and assessed during supervision.
Germany	• Yes, required.	• Yes, required for reporting from the management board to the supervisory board. • No required reporting among sub-committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • An appropriate report is required by specific risk information is not prescribed. • Reporting frequency is quarterly.	• No requirement to review the performance and skills needed on the board and risk committee. • No requirement to review the functions of the board's committee structure, but expected and assessed during supervision.
Hong Kong	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • Sufficient risk information is required to facilitate assessment of the risk appetite. Requirements cover risk MIS. • No minimum requirement on reporting frequency but the communication and reporting should be conducted regularly.	• Yes, reviews are required for both the performance and skills needed on the board and risk committee and the overall functions of the board's committee structure.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
India	• Yes, required.	• Yes, there is required reporting of key risk/concerns to board from the risk committee and among sub-committees. • Minutes of the risk committee are reviewed by the board and the minutes of the executive sub-committee by the risk committee.	• Yes, information is required to be in a standard form and contain certain minimum information. • Reporting frequency is not specified but critical concerns are required to be promptly escalated.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure. • Bank is required to provide training inputs for enhancing their performance.
Indonesia	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees. • Sub-committee members (if exist) shall consist of among other independent board members (commissioners). Hence reporting lines between risk monitoring committee to the board and among sub-committees exist by means of the membership of the independent board members in those committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • Required to provide information on overall risk level and information for each type of risk and each business unit. • Reporting frequency is quarterly.	• Yes, reviews are required for both the performance and skills needed on the board and risk committee and the overall functions of the board's committee structure. • Yes, reviews are required of the overall functions of the board's committee structure.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
Italy	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • Required to provide information on overall risk level and information for each type of risk and each business unit. • No reporting frequency is specified.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.
Japan	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be reported periodically and to contain certain minimum information. • Required to provide information on overall risk level and information for each type of risk and each business unit. • No reporting frequency is specified but in a regular and timely manner or on an as-needed basis.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.
Korea	• Not required, changes are under-way to make a requirement.	• No required reporting to/from the risk committee to the board and among sub-committees, but changes are underway to make a requirement.	• No information is required to be reported periodically and to contain certain minimum information. • No requirement to provide information on overall risk level and information for each type of risk and each business unit. • No reporting frequency is specified.	• No requirement to review the performance and skills needed on the board and risk committee or to review the functions of the board's committee structure, but a supervisory practice.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
Mexico	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, a set of minimum information requirements are outlined. • Yes, information on exposures, deviations and other aspects of consolidated risks, as well as for each unit and risk factor are required. • Reports to the risk committee are required monthly and to the board quarterly.	• No requirement to review the performance and skills needed on the board and risk committee. • No requirement for reviews of the overall functions of the board's committee structure, but a supervisory practice.
Netherlands	• Not required.	• Yes, reporting required from the management body to the supervisory board. • Yes, reporting required among sub-committees of the management body.	• Yes, information is required to be in a standard form and contain certain minimum information. • Yes, each key risk is required to be identified, properly managed and the holistic view reported. • Reporting frequency is 'regularly'.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.
Russia	• Not required, but best practices have been brought to the attention of firms.	• No required reporting, but best practices have been brought to the attention of firms.	• No requirement for risk information to be in a standard form, frequency or contain certain minimum information; but best practices have been brought to the attention of firms.	• No requirement to review the performance and skills needed on the board and risk committee nor to review the functions of the board's committee structure, but best practices have been brought to the attention of firms.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
Saudi Arabia	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be in a standard form, frequency and contain certain minimum information. • The level of detail is at discretion of board. • No reporting frequency is specified.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.
Singapore	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• Yes, information is required to be in a standard form, frequency and contain certain minimum information. • board is required to have sufficient understanding of each risk category. • Expect board to receive detailed information by risk type. • Frequency is 'regularly' but required to review the risk strategy at least annually.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.
South Africa	• Yes, required.	• No reporting required to/from the risk committee to the board and among sub-committees.	• No requirement for risk information to be in a standard form, frequency or contain certain minimum information. • board required to have sufficiently detailed information. • No reporting frequency specified.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
Spain	• Yes, required.	• No required reporting to/from the risk committee to the board, but supervisory practice. • No required reporting among sub-committees but required interactions among committees.	• No requirement for risk information to be in a standard form, frequency or contain certain minimum information, but firm's approach is assessed during supervision. • No requirements for level or type of risk information to provide, but firm's approach is assessed during supervision.	• No requirement to review the performance and skills needed on the board and risk committee or to review the functions of the board's committee structure, but a supervisory practice. • Changes are under-way to make a requirement.
Switzerland	• Not required, but a supervisory practice.	• Yes, reporting required to/from the risk committee to the board and among sub-committees. • No required reporting among sub-committees but a supervisory practice.	• Yes, information is required to be in a standard form and contain certain minimum information. • The type of level of risk information provided is at discretion of board. • Expect board to receive information on both overall risks and by type and business unit. • No reporting frequency is specified.	• Yes, reviews are required for the performance and skills needed on the board and risk committee. • No requirement to review the overall functions of the board's committee structure, but a supervisory practice.
Turkey	• Yes, required.	• No required reporting to/from the risk committee to the board. • Yes, required reporting for the audit committee and among different sub committees.	• Yes, information is required to be in a standard form and contain certain minimum information. • No reporting frequency is specified.	• Yes, reviews are required for both the performance and skills of the board and higher management.
United Kingdom	• Yes, required.	• Yes, reporting required to/from the risk committee to the board and among sub-committees.	• No requirement for risk information to be in a standard form, frequency or contain certain minimum information, but expect the board and CRO to ensure information is adequate.	• Yes, reviews are required for both the performance and skills of the board and risk committee and the overall functions of the board's committee structure.

Annex E: Regulatory and supervisory guidance – Governance of the board and sub-committees

	The board is required to set mandates and responsibilities of sub-committees	The board is required to have communication and reporting procedures:		The board and sub-committees are required to periodically review: (i) the performance, training and skills needed in the board and risk committee; and (ii) the functioning of the board's committee structure
		to/from the risk committee to the board and among different sub-committees	from the CRO to the board and risk committee (e.g., standard form, minimum information, type and level of information, frequency)	
United States	• Yes, required.	• No required reporting to/from the risk committee to the board or among sub-committees, but assessed during supervision.	• Yes, information is required for the audit committee. • Changes are in progress that may establish more specific requirements for the risk committee. • Supervisory guidance sets out expectations for risk reporting.	• No regulatory requirement to review the performance and skills needed on the board and risk committee or to review the functions of the board's committee structure, but assessed in practice. • NYSE Corporate Governance Guidelines require boards of publicly traded companies to conduct a self-evaluation at least annually to determine whether they and their committees are functioning effectively.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Argentina	• Yes, required for the risk management unit.	• Not required.	• No requirement for the CRO to have the ability to influence decisions that affect the firm's risk exposure but assessed during supervision. • No requirement to have access to information and to all relevant affiliates / subsidiaries.	• No requirement for the board/risk committee to communicate and meet with the CRO, but a supervisory practice. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but assessed during supervision. • No requirement for the CRO to interact regularly with the board, but assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Australia	• Not required, but expect the CRO to have operational independence and separation of responsibilities and reporting lines.	• Yes, required.	• No requirement for the CRO to have the ability to influence decisions that affect the firm's risk exposure but assessed during supervision. • No requirement to have access to information and to all relevant affiliates / subsidiaries, but is expected to have access.	• Yes, the board and the audit committee are required to have free and unfettered access to all senior management, including the CRO. • Yes, risk management functions must have free and unfettered access to the board and the audit committee in the absence of management. • No requirement for the CRO to interact regularly with the board, but regular interaction is expected. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Brazil	• Yes, segregation is required for the management of market, operational, liquidity, and credit risks.	• Not required, but expected to have technical skills and knowledge of risk management.	• No requirement to have access to information and to all relevant affiliates / subsidiaries, but is expected to have access.	• No requirement for the board/risk committee to communicate and meet with the CRO, but a supervisory practice (where a CRO is appointed). • No requirement for the CRO to meet with non-executive board members in the absence of senior management. • No requirement for the CRO to interact regularly with the board, but assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Canada	• Yes, required for all independent oversight functions.	• Not required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, unrestricted access is required for the board and risk committee • Yes, periodic meetings are required without senior management. • Yes, the minutes are assessed under the board assessment criteria. • Forthcoming guidance will require the risk committee to have input into the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
China	• Yes, required for both the risk management function and CRO.	• Yes, required.	• Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, the board and the audit committee are required to have access to the CRO. • Yes, the CRO can meet with non-executive board members in the absence of senior management when deemed necessary. • Yes, the risk management department shall regularly report to the board and these interactions would be recorded adequately. • Yes, the risk committee has a role in the appointment and dismissal of the CRO.
France	• Yes, the CRO is not able to perform any commercial, financial or accounting operation.	• Not required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, the board and the audit committee are required to have access to the CRO. • No requirement for the CRO to meet with non-executive board members in the absence of senior management. • No requirement for the CRO to interact regularly with the board, but assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Germany	• Yes, required for both the risk management function and CRO.	• Yes, required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, the board and audit committee are required to have access to the CRO; changes are in progress to strengthen requirements in the CRO's involvement in decision making. • No requirement for the CRO to meet with non-executive board members in the absence of senior management. • No requirement for the CRO to interact regularly with the board, but assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Hong Kong	• Yes, required for both the risk management function and CRO.	• Yes, required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, required for the risk management committee. • Yes, a direct reporting line is required. • Yes, regular interactions are required; changes are in progress to strengthen requirements around the recording of such interactions. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
India	• Yes, required for both the risk management function and CRO.	• Yes, required.	• Yes, the CRO is required to have the ability to influence decisions relating to market, operational and credit risks. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, required for the risk committee. • No requirement for the CRO to interact regularly with the board; however, CRO can interact with the board where deemed necessary. • No requirement for the CRO to interact regularly with the board; CRO's interactions with the board are when deemed necessary. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Indonesia	• Yes, required for both the risk management function and CRO.	• Yes, required.	• Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, board/risk committee can communicate and meet with the CRO. • Yes, in principle all members of board of Commissioners (including independent commissioners) may request a report from BoDs (including Risk Management Director - CRO) • Yes, risk management unit is required to submit periodic risk profile report to board of Directors (at least quarterly) and board of Commissioners may request a report from CRO • The risk monitoring committee monitors and evaluates the performance of the risk management committee and risk management unit (including the CRO) and provides recommendation to the board members (commissioners), which may include recommendation regarding the appointment and dismissal of the CRO.
Italy	• Yes, required.	• Not required but expected to have technical skills and knowledge of risk management.	• No requirement for the CRO to have the ability to influence decisions that affect the firm's risk exposure but changes are underway. • No requirement for the CRO to have the ability to have access to information and to all relevant affiliates / subsidiaries, but changes are underway.	• No requirement for the board/risk committee to communicate and meet with the CRO, but changes are underway. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but changes are underway. • No requirement for the CRO to interact regularly with the board, but assessed during supervision, but changes are underway. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Japan	• Yes, required for the risk management function.	• Yes, required.	• Yes, the risk management function is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the risk management function is required to have the ability to have access to information and to all relevant affiliates / subsidiaries	• Yes, unrestricted access is required for the board and risk committee. • Yes, the risk management function can meet with non-executive board members in the absence of senior management. • Yes, regular interactions are required and interactions are expected to be recorded adequately. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Korea	• Yes, required for the risk management function.	• Yes, required.	• No requirement for the CRO to have the ability to influence decisions that affect the firm's risk exposure but assessed during supervision. • No requirement to have access to information and to all relevant affiliates / subsidiaries, but is expected to have access.	• No requirement for the board/risk committee to communicate and meet with the CRO, but a supervisory practice; changes are in progress to make a requirement. • No requirement for the CRO to meet with non-executive board members in the absence of senior management. • No requirement for the CRO to interact regularly with the board, but assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Mexico	• Yes, required for all the risk management function personnel.	• Yes, required.	• No requirement for the CRO to have the ability to influence decisions that affect the firm's risk exposure but, as a member of the risk committee, the CRO has such influence. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, required and facilitated by the CRO being a member of the risk committee. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but facilitated by the CRO being a member of the risk committee. • No requirement for the CRO to interact regularly with the board, but facilitated by the CRO being a member of the risk committee, which is required to meet at least monthly and have its agreements set out in the minutes. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Netherlands	• Yes, required for the risk management function and CRO.	• Yes, required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, unrestricted access is required for the board and risk committee. • Yes, the risk management function can meet with non-executive board members in the absence of senior management. • Yes, regular interactions are required and interactions are expected to be recorded adequately. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Russia	• Yes, in the context of risk management personnel being subject to conflict of interest requirements.	• Not required, but best practices have been brought to the attention of firms.	• Not required, but best practices have been brought to the attention of firms.	• No requirement for the board/risk committee to communicate and meet with the CRO, but best practices have been brought to the attention of firms. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but best practices have been brought to the attention of firms. • No requirement for the CRO to interact regularly with the board, but best practices have been brought to the attention of firms. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Saudi Arabia	• Yes, required.	• Yes required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, unrestricted access is required for the board and risk committee. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but in most cases the CRO can meet with the board in absence of senior management. • No requirement for the CRO to interact regularly with the board, in most cases the CRO can interact with the board, usually through the risk committee, credit approval or ICAAP process. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Singapore	• Yes, required.	• Yes, required.	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure, including by requiring the CRO to be a member or chair key management committees. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, unrestricted access is required for the board and risk committee as the CRO is required to be a member or chair key management committees. • Yes, the CRO is required to have a direct reporting line to the board • Yes, the CRO is required to interact regularly with the board and is able to do so in absence of senior management and minutes are drafted. • Yes, the risk committee approves the appointment, dismissal and performance evaluation of the CRO.
South Africa	• Yes, required.	• Yes, required	• Yes, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, requirements exist for the board/risk committee to communicate and meet with the CRO. • Yes, requirements exist for the CRO to meet with non-executive board members in the absence of senior management. • Yes, requirements exist for the CRO to interact regularly with the board. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Spain	• Yes, required.	• Not required.	• No requirement for the CRO to have the ability to influence decisions that affect the firm's risk exposure, but a supervisory practice. • No requirement for the CRO to have access to information and to all relevant affiliates / subsidiaries, but a supervisory practice.	• No requirement for the board/risk committee to communicate and meet with the CRO, but a supervisory practice. • No requirement for the CRO to meet with non-executive board members in the absence of senior management. • No requirement for the CRO to interact regularly with the board. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.
Switzerland	• No requirement, but expect the CRO to be independent.	• Yes, required.	• No requirement but an expectation for the CRO to have the ability to influence decisions that affect the firm's risk exposure; also expect the CRO to be senior enough to have impact within firm. • No requirement for the CRO to have access to information and to all relevant affiliates / subsidiaries, but a supervisory expectation.	• No requirement for the board/risk committee to communicate and meet with the CRO, but a practice assessed during supervision. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but a practice assessed during supervision. • No requirement for the CRO to interact regularly with the board, but a practice assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
Turkey	• Yes, required for banks and broker-dealers.	• Yes, required.	• Yes, the risk management unit and the unit's manager are required to have the ability to influence decisions that affect the firm's risk exposure.	• Yes, requirements exist for the board/risk committee to communicate and meet with the CRO. • No requirement for the CRO to meet with non-executive board members in the absence of senior management. • No requirement for the CRO to interact regularly with the board. • Yes, the board is responsible for deciding the selection and removal of the managers of the units included within the scope of the internal systems (internal control, internal audit and risk management systems).
United Kingdom	• Required for the risk management function where nature, scale and complexity makes it appropriate.	• Yes, required.	• Yes, CRO should alert governing body to, and provide challenge on, any business strategy or plans that exceed the firm's risk appetite and tolerance.	• Yes, requirements exist for the board/risk committee to communicate and meet with the CRO. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but a practice assessed during supervision. • No requirement for the CRO to interact regularly with the board, but a practice assessed during supervision. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex F: Regulatory and supervisory guidance – the CRO and risk management function

	Independence *be distinct from other executive and revenue-generating functions and business line responsibilities*	**Qualifications** *Fit and proper tests*	**Authority** *have the ability to influence decisions that affect the firm's exposure to risk*	**Stature** *(i) the board/risk committee can communicate and meet with the CRO; (ii) the CRO can meet with non-executive board members in the absence of senior management; (iii) the CRO interacts with the board regularly and these interactions be recorded adequately; (iv) the risk committee has a key role in the appointment and dismissal of the CRO*
United States	• Yes, required for large banks (under heightened expectations).	• Yes, required.	• Yes, for large banks, the CRO is required to have the ability to influence decisions that affect the firm's risk exposure. • Yes, the CRO is required to have the ability to have access to information and to all relevant affiliates / subsidiaries.	• Yes, requirements exist for the board to communicate and meet with the CRO. Changes are in progress that may establish more specific requirements for the risk committee. • No requirement for the CRO to meet with non-executive board members in the absence of senior management, but, for large banks, heightened expectations exist for the CRO to meet with the board absent senior management. • No requirement for the CRO to interact regularly with the board, but, for large banks, heightened expectations exist for the CRO and the board to meet regularly. • No requirement for the risk committee to have a key role in the appointment and dismissal of the CRO.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Argentina	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • No specific requirement for compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee and the head of audit sits on the audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least annually.	• No escalation process is in place or foreseen. • However, the BCRA investigates reports of irregular situations made by employees or the general public, even those that are submitted informally.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.
Australia	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee. Any reporting line that would call into question independence is precluded. • Yes, required to report findings directly to the board and/or audit committee.	• No requirement for specific frequency of assessments or testing functions, but expected to reflect the risk of the business function and occur on a regular cycle.	• Yes, require financial institutions not to, in any way, impede or constrain persons from disclosing information to APRA, to any auditor or to any other person who has statutory responsibilities in relation to the regulated institution. • Legislation also contains protections for whistle blowers.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Brazil	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the board and/or audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least half yearly.	• Not required in the course of supervisory activities; an escalation process is not mandatory for the communication of specific situations or behaviours within a firm.	• Yes, the board/risk committee are required to have access to external expert advice, but it is expected that internal audit activity be performed by a specific unit within a financial institution, especially at relevant ones. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Canada	• Yes required to be a permanent function depending on the size, but expect to exist for large and complex banks. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Not required, but for large, complex firms, the CAE should report to the CEO for administrative purposes, and to the audit committee chair for functional purposes. • Forthcoming guidance will require the CAE to have sufficient stature and authority within the organisation, be independent from operational management, have unfettered access, and for functional purposes, a direct reporting line to the board and audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required.	• Firms have established whistle-blower hotlines which provide an opportunity for an individual within a firm to communicate matters to the supervisor.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
China	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, the chief auditor and the internal audit department shall report directly to the board. • Yes, required to report timely findings directly to the board and/or audit committee.	• Yes, required at least bi-annually.	• No formal escalation processes are required but any person within a firm can report firm deficiencies to the supervisor. The supervisor would conduct reviews if deemed necessary and give individuals appropriate feedback.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.
France	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• No, generally report to the CEO. • Not required to report findings directly to the audit committee.	• Yes, required.	• Yes, firms are required to have an escalation process in place and appoint a compliance officer to collect within the firm any relevant information and to transmit this information to the ACP.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Germany	• Yes, required to be a permanent function, which may be undertaken by a member of the management body if the size of the firm permits. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the board and/or audit committee. • Yes, required to report findings directly to the management board.	• Yes, required within at least three years or at appropriate intervals.	• Not currently required, but in the future, the banking act will introduce escalation processes such as whistle-blowing. • The draft version requires institutions to have processes that enable employees to anonymously report breaches and criminal behaviour within the firm. • In addition, BaFin will establish a whistle-blowing scheme in order to receive breaches.	• No, the board/risk committee are not required to have access to external expert advice, but is a supervisory expectation. • Yes, third parties are required to report findings to the board.
Hong Kong	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the board and/or audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required.	• Yes, firms are required to have an escalation process in place.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
India	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • No specific requirement for compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee. • Yes, required to report findings directly to the audit committee; critical concerns may be reported directly to the board.	• Yes, required and the frequency is specified by the internal audit policy and the risk rating of the activity /location to be assessed. • Risk assessment is required to be carried out once a year. • Adequacy of risk limits and breaches are also examined during specific audits.	• Yes, firms are required to have an escalation process in place. • Banks are required to have policies and procedures in place to protect disclosure of whistle blowers.	• No requirement for the board/risk committee to have access to external expert advice, but not precluded where deemed necessary. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Indonesia	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is supported by compensation or career plans. The position of Chief of Internal Auditors in the organization chart must be set in such a way so that he/she can express his/her views and thoughts without the influence of pressure from management or any other parties. Moreover, remuneration and nomination policies are reviewed by a committee consisting of among others independent board members (commissioners).	• Yes, Internal Audit required to report directly to the President director and the chair of the board. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least annually.	• Yes, banks are required to have a commitment to provide support and protection to whistle blowers and ensure secrecy of the respective whistle blower's identity and fraud report submitted.	• Yes, the board/risk committee have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Italy	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit is required to report directly to the board. • Yes, required to report findings directly to the board and the internal control committee, where established.	• Yes, required at least annually.	• Not currently required, but in the future, new regulation will introduce escalation processes such as whistle blowing.	• The use of third parties is not regulated. • As a general principle, banks are not allowed to outsource the responsibilities of the internal audit function; only small credit institutions can.
Japan	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the board and/or audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least annually.	• Yes, firms are required to have points of contact in place for whistle blowing and consultation.	• Yes, the board/risk committee are required to have access to external expert advice and third parties. • No, the use of third parties is not regulated.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Korea	• Not required to be a permanent function, but expected. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• No, Internal Audit not required to report directly to the board and/or audit committee but recommended. • Not required to report findings directly to the audit committee but recommended.	• Yes, required at least annually.	• Yes, firms are required to have an escalation process in place.	• No requirement for the board/risk committee to have access to external expert advice, but changes are underway. • No, use of third parties is not regulated.
Mexico	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least annually.	• Not required to have an escalation process in place.	• Yes, the board/risk committee are required to have access to external expert advice and third parties. • No, use of third parties is not regulated.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Netherlands	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit is required to report directly to the management body and/or audit committee. • Yes, required to report finding to the management body and/or audit committee on areas for improvement.	• Yes, required at least annually.	• Yes, banks are required to report serious incidents and compliance breaches. • In addition, many institutions have put a whistle-blower procedure in place. Escalation procedures are in place for some control functions, such as the internal auditor who can address their concerns directly to the chair of the supervisory board.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.
Russia	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, supervisor evaluates whether compensation scheme for internal audit is approved by the board (effective from 01.07.2013).	• Yes, Internal Audit required to report directly to the audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required.	• Not required but any person can report an abuse to the supervisor. No specific procedure is envisaged for individuals within a firm.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Saudi Arabia	• Yes, required to be a permanent function. • Yes, required to be independent from risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required.	• Not required, but banks are expected to put risk management procedures in place for communication of specific situations and behaviour within a bank to SAMA.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.
Singapore	• Yes, required to be a permanent function. • Yes, required to be independent from risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least annually.	• Not required, but there are open channels available for individuals to communicate with MAS. All feedback would be reviewed and follow-up could include MAS investigating the allegations, as well as directing the firms to conduct an independent review.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
South Africa	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required.	• Yes, firms are required to have an escalation process in place.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.
Spain	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • No specific requirement for compensation and career plans but broadly expected.	• No, Internal Audit not required to report directly to the board and/or audit committee. • Not required to report findings directly to the board and/or audit committee.	• Yes, required.	• Not required to put in place escalation processes; however, practices exist within institutions. Whistle blowing by individuals to supervisors is not regulated.	• Yes, the board/risk committee are required to have access to external expert advice. • No, use of third parties is not regulated.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
Switzerland	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Not required but Internal Audit expected to report directly to the board and/or audit committee. • Yes, required to report findings directly to the board and/or audit committee.	• Yes, required at least annually.	• Not required, but banks are expected to have a process in place.	• No requirement for the board/risk committee to have access to external expert advice, but supervisory expectation. • Yes, third parties are required to report findings to the board.
Turkey	• Yes, required to be a permanent function. • Yes, required to be independent from the risk management function. • Yes, independence is required to be supported by compensation and career plans.	• Yes, Internal Audit required to report directly to the board and audit committee. • Yes, required to report findings directly to the relevant board member	• Yes, required.	• Yes, suitable communication channels must be established and maintained to ensure that problems encountered by bank personnel are reported to the management levels in their own units.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
United Kingdom	• Yes, required where appropriate and proportionate in view of the nature, scale and complexity of the business, and nature and range of its financial services and activities. • Yes, required to be independent from the risk management function. • No specific requirement for compensation and career plans but broadly expected but expect the head of internal audit to be covered by Remuneration Code.	• No, Internal Audit not required to report directly to the board and/or audit committee but recommended (applying the proportionality principle).	• Yes, required at least annually.	• Not required but supervisory guidance sets out how firms may consider setting up appropriate internal procedures which will encourage workers with concerns to blow the whistle internally about matters which are relevant to the functions of the UK FSA.	• Yes, the board/risk committee are required to have access to external expert advice. • Yes, third parties are required to report findings to the board.

Annex G: Regulatory and supervisory guidance – the internal audit function

	Independence *(i) be permanent function; (ii) distinct from the risk management function; and (iii) supported by compensation or career plans*	**Stature** *(i) reports directly to the board and/or audit committee; and (ii) reports its findings directly to the board and/or audit committee*	**Independent assessment** *Required to conduct assessment and testing functions at a specific frequency*	**Escalation processes** *Required to be in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (e.g., whistle-blowing)*	**Third parties** *The board/risk committee have access to external expert advice and third parties report findings to the board*
United States	• Yes, required to be a permanent function. • Yes, required to be independent from risk management function. • Yes, under heightened expectations, compensation plans should be structured to promote behaviour appropriate for audit's role/responsibilities and to attract/retain talent commensurate with business counterparts. • No expectation directly linking independence to career paths.	• Not required but supervisory guidance encourages reporting to the board audit committee on both administrative issues and audit findings.	• Yes, required at least annually.	• Yes, all audit committees of institutions that are subject to SOX are responsible for handling complaints and confidential employee concerns (whistle blowing). • As part of the mandated audit committee function, publicly traded corporations must also establish procedures for employees to file internal whistle-blower complaints, and procedures which would protect the confidentiality of employees who file allegations with the audit committee.	• No requirement for the board/risk committee to have access to external expert advice, but not precluded. • Yes, third parties are required to report findings to the board.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Argentina	• Approximately every 18 months through on-site inspections which occur within its continuous supervision cycle. • Conclusions feed into the risk-based rating system (CAMELBIG).	• Board and senior management reports. • Corporate governance policies. • Strategic objectives and corporate values. • Committees and working groups. • Reports issued by various functional areas and commissions.	• External auditor's risk management reports (with their scope and conclusions), along with all supporting documentation to enable the supervisor to evaluate the changes being carried out in the institution.	• Board • Senior Management
Australia	• Regular reviews of all regulated institutions. • Regular on-site visits to regulated institutions. • Risk-based supervisory approach.	• Capital, market, liquidity, operational and market risk reports. • Ad-hoc reports on areas of concern of firm's operations/practices.	• Matters relating to APRA data collections. • Reviews of internal controls.	• Board • CEO • CRO • Risk managers
Brazil	• Annual comprehensive risk and controls assessment for financial institutions deemed relevant and bi-annually for others.	• Risk management structure for credit, market and operational risks in financial statements. • Audit committee assessment of the internal control system, including risk management. • For publicly traded companies, information about their risk management structure and policies for market risk.	• Quality and adequacy of the internal controls system from external audit, including risk management structures.	• Board • Risk committee • Audit committee • Risk managers • Senior management • Technical staff

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Canada	• Continuous supervision. • Risk-based supervisory framework. • Quarterly monitoring processes which include work, meetings, and assessments undertaken by the institution-specific supervisory team, and the Supervision Support Groups including the Corporate Governance Division. • Ability to respond to ad hoc requests from OSFI, such as data / information requests on particular risks and exposures. • Specialised reviews (e.g., corporate governance).	• Board and Committee packages. • Management reports, including the CRO's reports to the board, risk committee and senior management as well as reports from the CAE, CFO, CCO. • Risk management policies, authorities, limits. • Risk appetite framework. • Strategic documents – enterprise-wide and by business unit level. • New product and initiative frameworks and supporting documentation when utilised. • Mandate, budget, resources, organisational charts. • Internal audit reports relating to risk management areas. • Specific reports by risk type (e.g., trading, credit). • Credit specific reports, such as portfolio data and credit metrics. • Special ad hoc reports on topics of interest (e.g., municipal bonds).	• External auditors working papers, which includes the scope documents, matters for partner attention, etc. • Quarterly meetings with the assigned external audit partners to discuss a variety of topics, including risk management practices. • Where the firm has undertaken third party/external reviews, copies of the scope document and the report. • Meetings with the consultant to get a better understanding of their work, findings/recommendations, etc.	• Chair of the board • Chairs of the audit and risk committees • The board • President and CEO • Chief audit executive and direct reports • Chief financial officer and direct reports • Chief compliance officer and direct reports. • CRO and direct reports. • Various individuals on the business side and the appropriate level of individuals on the oversight function, which almost always include risk management staff.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
China	• On-going supervision involving continuous off-site supervision and on-site examination. • Annually or irregularly as needed.	• Various risk statements on a monthly, quarterly, semi-annual and annual basis, as well as certain daily risk reports.	• Audit reports and management proposals.	• The board and senior managers.
France	• Continuous supervision for all major banks and significant or specialised subsidiaries of foreign banks.	• Annual report on risks. • For large banks, board and audit committee reports, as well as risk committee presentations on a quarterly basis.	• When used in the risk management process, third parties' reports are examined by the ACP in the same way internal audit reports are reviewed.	• All hierarchical levels within the bank.
Germany	• At least once a year. • Continuous supervision for all major banks and significant or specialised subsidiaries of foreign banks.	• In general, off-site supervision collects and analyses information based on the annual financial statements. • Ad hoc reports if certain circumstances or events require further information for supervision (e.g., reports from internal audit, risk reports). • As a result of the audit (on-site supervision), reports are written and provided to off-site supervisors of BaFin and Bundesbank.	• External auditors are responsible for the annual financial report, which is provided to the Bundesbank. • Ad hoc reports / information can be made available by the institution itself or by third parties. In this context it is up to the institution to mandate external consultants / auditors. • BaFin itself can authorise external auditors to carry out audits on certain topics. The results of the audit are provided in a report to the Bundesbank and BaFin.	• For off-site supervision, BaFin and the Bundesbank expect the management board to meet supervisors on, at least, an annual basis. • When the Bundesbank carries out audits in the context of on-site supervision all relevant persons in an institution can be involved, including the board and CRO.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Hong Kong	• On-going risk-based supervision involving a process of continuing off-site supervision which is complemented and strengthened by on-site examinations, prudential interviews (at least annually), and supervisory meetings with boards/ specialised committees (at least annually for locally incorporated authorised institutions, and on an ad-hoc basis when necessary). • The assessment of the adequacy of the overall risk management policies and practices is rated and reflected in the CAMEL rating review and the Pillar 2 SRP of individual authorised institutions, which are done at least annually.	• Board-level and senior management committees structure, and their terms of reference. • Business plans and lists of new businesses, products or services. • Information packs for the board and its sub- committees (e.g., ALCO pack). • Organisational structure of the risk management function. • Risk management framework and risk appetite assessment. • Policies and procedure manuals. • Internal management information system (MIS) reports. • Stress testing procedures and results. • Plans and reports of internal audit and compliance review.	• Independent assessment reports for any ad hoc reviews on control systems in areas such as corporate governance, risk management and controls relating to specific operational areas, loan classification system, information technology, business continuity planning, prevention of money laundering, and internal audit. • External auditors' management letters, which include any material internal control weaknesses identified during the course of their audit and recommendations for improvement. • Auditors' reports on the adequacy of the authorised institutions' control systems over the compilation of banking returns or other information, and compliance with certain statutory provisions. • Auditor's reports on matters that, in their opinion, adversely affect the firm's financial position to a material extent, or constitutes a failure to comply with certain provisions or rules made under the Securities and Futures Ordinance.	• Hold annual prudential meetings with senior management, including the CRO and CEO, to convey views on the overall risk management system and any matters of prudential concern. • For locally incorporated authorised institutions, annual meetings with their board or specialised committees (e.g., audit committee). • In addition to the prudential meetings, meet with the CRO and /or senior risk management personnel from time to time to discuss specific issues relating to the firm's risk management policies and practices. • The above requirements are applicable to all authorised institutions regardless of their size and complexity of operations.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
India	• Continuous supervision through off-site monitoring through structured returns and on-site inspections. • SIFIs and banks warranting closer supervision as per their risk profile are examined/ inspected once a year. Other banks are inspected at least once in two years. • Conclusions feed into the risk-based rating system (CAMELS), which also assesses the adequacy of their risk management policies and procedures.	• Annual ICAAP report. • Quarterly Risk Profile Templates, risk reviews, and stress testing results. • Audited annual accounts. • Reports and minutes of the board and its sub-committees (e.g., risk and audit committees, ALCO meetings). • Policy guidelines, business strategy. • Document and review thereof by board. • Internal audit reports. • Regulatory reporting on compliance with inspection reports and compliance with remediation plans based on supervisory findings. • Host supervisor's examination reports of overseas branches of Indian banks.	• Long Form Audit Reports from statutory auditors and reports of concurrent auditors. • Forensic Audit Reports. • Independent audit by auditor appointed by the RBI to examine specific areas/concerns. • Actuarial assessment of certain liabilities. • Supplemented by interactions with bank's statutory auditors where required.	• Chair of the board • CEO and Managing Directors • CRO (on-site inspection process) • Independent directors and chair of the audit committee, particularly to discuss findings of supervisory examinations. • Periodic discussions with top management. • Heads of various key committees and business units, including, where required, with direct dealing officials. • Supervisory meetings are periodically conducted with bank's top management.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Indonesia	• At least once a year is required, but in practice, is generally on average twice a year, for different activities (e.g., credit risk, operational risk) in accordance with the Supervisory Plan defined at the beginning of the year. • The length of time, the amount of resources and necessary expertise to conduct the examination is based on size, complexity, and systemic considerations. • Supervisory and examination approach for SIFIs is not that different compared to other banks. However, monitoring is done more frequently.	• *Periodic reports/data:* Financial reports/ data, Bank's Annual Business Plan Report, Semester Report on Compliance Functions, Quarterly Risk Profile and CAMELS report, Semester Report on Internal Audit, Internal Audit Review Report (every 3 years), Core Debtor and Depositor Report, Wealth Management Product Portfolio Report. • *Non-periodical reports/data:* IT Development Report, Product and New Activity Plan Report, Market Entry Plan Report, and additional data required by supervisors such as a particular stress tests, treasury activities. • Internal Audit Examination Result, bank's internal policy and procedure, board and sub-committee meeting minutes.	• Reports from third parties, in particular Audit Reports and Management Letters submitted by external auditors. Third party examination report by other authorities on a bank's branches in other jurisdictions.	• Board members, bank senior-level officers, technical officers of the bank. • High level meetings are carried out during examination exit meeting. • Meetings with the board to discuss matters of supervisory concern, the business plan which, among others, highlights risk management implementation aspects, and risk appetite. • In the case of a problem bank, meetings are carried out more intensively based on supervisory needs, particularly in relation to progress on completing the remediation action plan.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Italy	• The risk management framework is assessed, on a regular basis, once a year. The evaluation is reflected within the rating assigned to the "governance and internal control system profile" within the RAS assessment. Evaluations are updated when new information becomes available. • The risk management framework is also examined during on-site inspections and internal models assessments, both conducted in accordance with plans defined at the end of each year. • Additional ad-hoc examinations are conducted whenever necessary for specific needs (e.g., market developments, new regulations).	• ICAAP report. • Corporate governance report. • Pillar 3 report. • Internal reports from risk management, compliance and auditors. • Balance sheet.	• For major institutions, reports from accounting auditors and rating agencies.	• The board • CRO and risk managers

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Japan	• On an annual basis, firm interviews are conducted to check issues such as the firm's risk management status, issues, and policies. Additional interviews are conducted when necessary on market trends and other developments. • For major banks, conduct on-site inspections approximately once a year.	• Authorities have meetings to hear about the current risk management, tasks and future plans once a year. Also, additional meetings are held as needed, taking into account market development. • Authorities request financial institutions to report regularly about risk management information.	• When conducting on-site inspections of financial institutions, the FSA, if necessary, refers to the results of external audits and exchanges views with the institution's accounting auditors.	• On- and off-site interviews with various levels of officers of financial institutions, whenever necessary, including non-executive and executive levels.
Korea	• Risk-based supervision (RADARs) conducted every six months.	• Major reports on risk management such as risk committee meeting records whenever necessary.	• Audit reports on risk management from the external auditor.	• Risk managers and working level staff.
Mexico	• Evaluations are made annually to the 7 main banks and to other banks according to our risk-based supervision methodology and risk matrix (CEFER).	• Risk management reports on the firm's risk exposure, incidence levels and impact, as well as a description of risks, causes and consequences. • Fulfilment level of objectives, guidelines and policies, audit review or evaluations. • Cases in which either the risk exposure limit or tolerance level were exceeded.	• Institutions should give the CNBV the external audit's report, including consolidated financial statements and notes, opinions, reports and all communications the external auditor emits. • The CNBV could ask both, the institution and the external auditor, for additional information.	• Although senior management is responsible for the implementation of risk management and internal control systems, CNBV meets with all relevant personnel, independent of their seniority.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Netherlands	• Once a year based on the risk assessment and updated when actual information (i.e., on implementation of remedial actions or changes in business model) are available.	• A great variety depending on the type of business. • Many risk reports from the risk management function itself. • Reports from control functions.	• Reports from the rating agencies and reports from external auditors.	• Frequent meetings with board members, the CRO and direct reports, and risk managers with oversight responsibilities, based on supervisory programs derived from risk assessments.
Russia	• Quarterly as set out in regulation.	• Business-plans, annual reports, quarterly securities issuer statements, reports on internal controls, filings on credit, market, liquidity, foreign exchange and other risks. • Strategy statements, internal documents, internal auditor reports, board minutes, orders of executive bodies, corporate governance self-assessment results.	• External Auditor's Statement, which should include auditor's opinion on the quality of management and internal controls.	• Regulation specifies that representatives and resident supervisors may contact the CEO and direct reports, executive board members, internal control staff, and branch managers, business-line managers and other employees.
Saudi Arabia	• Continuous risk-based supervisory process. • Onsite inspections are performed on a regular basis.	• A variety of reports on risks through its prudential reporting system. • Collects reports on various risks during the annual ICAAP process and during its supervisory visits and inspections, which include information on credit risk (e.g., large exposure, concentration risk, counter parties, provisioning), market, operational, foreign exchange, interest rate, and reputation risks.	• External auditors provide a report on weaknesses through their annual management letters and can meet with supervisors to share their views on identified weaknesses.	• Board members • CRO • Risk managers with oversight responsibilities

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Singapore	• Evaluations of the robustness of the banks' risk management framework are conducted regularly and at least annually as part of both off-site and on-site supervisory reviews. • Observations from these reviews as well as interactions with the banks culminate in the annual supervisory assessment.	• Monthly and quarterly regulatory returns as well as discussion on significant risk matters tabled at the banks' board and management level risk committee meetings (such as Market risk committee, Operational risk committee, Credit risk committee, Asset-Liability Committee). For instance: o Discussion material on ICAAP and the corresponding discussion minutes; o Quarterly returns, which contains detailed information of the bank's capital position and credit exposures respectively; o Internal audit reports on the reviews relating to ICAAP, stress testing frameworks and processes and risk management and internal controls.	• External auditors are required to provide their assessment of the banks' risk management policies, including: o a copy of the auditor's long form report, which includes the auditor's findings and recommendations on internal controls, quality of loans and advances and other assets, and any non-compliance with the legislation, regulations, guidelines and circulars issued by the MAS, or any other relevant laws and regulations; and o regular reports on discussions at audit committee meetings, which include the auditor's observations and recommendations for that quarter, as well as other updates deemed significant to be highlighted to the audit committee. • Other reviews that the external auditor or other external consultants are commissioned to conduct, either by the bank or other regulatory authorities.	• Interactions at various levels of seniority, including board members, CRO and his direct reports, and risk managers. o Meet locally incorporated banks' board members both as a group during the annual supervisory meeting, as well as individually in other forums. o Meet regularly with the CRO and direct reports, and risk managers, separately or as a group for updates on matters relating to the risk management function and risk profile of the bank. In addition, ad-hoc meetings with the CRO as necessary, such as for discussions on significant initiatives that would have an impact on the risk profile of the bank. o Meet risk managers during on-site inspections to understand processes relating to the respective risk management areas.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
South Africa	• At least annually for banks with approval to report their risk-weighted assets or operational risk according to a modelled method. • Appropriateness of risk management policy and practice is usually assessed in conjunction with the banks' internal audit functions.	• Not provided	• Not provided	• Prudential meetings are held on an annual basis with individuals on all levels of seniority within the bank, including board members, CEO, and executive officers.

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Spain	• Multiple tasks comprising the supervisory process enable to update as often as necessary, but at least annually, each institution's supervisory risk profile and, where applicable, supervisory strategy and plan for the institution.	• ICAAP report. • Internal management information provided by institutions during on-site and continuous monitoring, e.g., presentations for the board and sub-committees. • A required public report which contains information on risk management goals, policies, strategies, processes and structure of the function. • Entities must submit an annual report on corporate governance, which should facilitate, among other information, relating to risk control systems, whose content is regulated.	• Generally not of an obligatory nature, except in some sections of the supplementary audit report relating to specific aspects of internal control, where any weaknesses detected must be included in a Comments Letter written by the auditors and addressed to management of the institution. • Such specific reports by external auditors as may be known are requested from the institutions.	• The existing supervisory powers place no limitations on the nature of the people at institutions with whom meetings may be held. It depends on the complexity and size of the institutions, but at large institutions meetings with board members are not usual; rather, they tend to be with management committee members or risk managers. • The Securities Exchange Act regulates the powers of the CNMV for the supervision and inspection of listed companies, which may involve requiring meetings with the supervisee.
Switzerland	• Continuous supervision of large- and medium-sized banks as well as problematic institutions. • Risk management policies and practises are also assessed by external auditors on an annual basis.	• Policy changes. • Risk, liquidity and capital planning. • For the medium-sized banks, quarterly reporting is standardised and complemented by ad hoc information. • Extent to which risk functions are involved in remuneration system oversight.	• Annual reports of their assessment (i.e., long form report). • On an ad hoc basis, external auditors can be asked to conduct reviews of specific areas and in-depth audits.	• Board members • Executive board members • Other senior managers • CRO and director reports • Other heads of business units

Annex H: Supervisory approach toward assessing firms' risk management framework

	Type and frequency of supervisory evaluations	Types of reports or information collected from firms on their risk management practices	Types of reports or information collected on firms' risk management practices from third parties	Seniority of individuals you meet with at the firm
Turkey	• Primarily once a year.	• Internal control and risk reports. • Internal audit and risk management reports. • Strategy and policy documents. • Risk profile and risk limits. • Board and management reports. • Minutes for board meetings.	• Independent audit reports. • General economic reports. • Reports on the banking sector and real sector.	• Chair of the board • Board members • General manager • Audit committee members • Head of risk management • Other risk practitioners
United Kingdom	• Depends on size, nature and complexity of the firm. • Every two years currently, but moving toward a system of continuous assessment.	• Governance and risk management policies. • Board and sub-committee terms of reference and minutes. • Risk committee management information packs. • Individual job descriptions. • board effectiveness reviews.	• Board effectiveness reviews. • Specific reports produced.	• Chair of the board • Executive board members • Non-executive board members • Members of the senior management team (including the C-Suite) • Risk managers
United States	• Continuous supervision and targeted exams. • Quarterly evaluation and reports on each element of the risk management framework (through the risk assessment system) and through a core assessment on an annual basis.	• Board packages. • Management reports. • Internal audit reports. • Various reports on risks, revenues, costs, strategies as well as outstanding concerns and the status of corrections.	• Examination staff review reports provided to management by third parties, such as external auditors and consultants.	• CEO and direct reports down 2-3 levels • CRO and direct reports down 1-2 levels • CAE and direct reports down 1-2 levels. • Board members (bank and holding company) and key committees, particularly the chair of the audit committee.