3 April 2012

Thematic review on risk governance

Questionnaire for national authorities

The global financial crisis highlighted a number of corporate governance failures and weaknesses in financial institutions, including inappropriate Board structures and processes, weak risk governance systems, and unduly complex or opaque firm organisational structures and activities. Many of these shortcomings have been highlighted and documented in various reports that have been issued since 2008.[1]

The October 2011 FSB Supervisory Intensity and Effectiveness (SIE) progress report to the G20 notes that much progress has been made in corporate governance at both the supervisory and firm levels, particularly for SIFIs. However, effective risk appetite frameworks that are actionable and measurable by both firms and supervisors have not yet been widely adopted. The SIE report concludes that more intense supervisory oversight is needed to evaluate the effectiveness of improved governance, particularly risk governance that is critical to ensuring a strong risk management culture in firms. The report recommends that the FSB conduct a thematic review on risk governance to assess practices at firms, focusing on the risk committees of executive Boards, as well as the risk management functions (e.g. the Chief Risk Officer organisation) and independent assessment functions (e.g. the Chief Auditor function), and on how supervisors assess their effectiveness.

In light of the recommendation of the SIE report, and the importance and cross-sectoral nature of the topic, the FSB Standing Committee on Standards Implementation (SCSI) agreed, in its conference call on 10 November 2011, to undertake a peer review on risk governance in early 2012. SCSI members also agreed that the peer review would only cover banks and broker-dealers; insurers and other non-bank financial institutions would not be covered.

There is currently no single comprehensive set of principles and standards that fully address and integrate corporate and risk governance requirements. The review therefore will not assess compliance with any specific standard, but will use existing standards[2] and recommendations (as appropriate) in order to evaluate progress as well as identify good practices and remaining gaps in firms' risk governance frameworks, and in the assessment of those frameworks by supervisory authorities.

---

[1] 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), and *Corporate Governance in Financial Institutions: Lessons to be drawn from the current financial crisis, best practices* by the European Commission (June 2010).

[2] BCBS *Principles for Enhancing Corporate Governance*; OECD *Principles of Corporate Governance*; and BCBS *Internal Audit with Banks and the Supervisor's Relationship with Auditors.*

The primary source of information for the peer review will be the responses provided to this questionnaire, and a questionnaire for firms to be developed in March.

The peer review will focus on the roles and interplay between the firm's Board members that oversee risk management, the enterprise risk management function and relevant aspects of the process for assessing the risk governance framework, processes and practices, either by internal audit or by third parties (e.g. external auditors, consultants). In particular, the peer review will focus on:

- *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. How Boards assume such responsibilities varies across jurisdictions and for the purposes of this report, the risk committee refers to a specialised Board committee responsible for advising the Board on the firm's overall current and future risk appetite and strategy, and for overseeing senior management's implementation of that strategy.[3]
- *Risk management function*: 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.
- *Independent assessment of the risk governance framework by internal audit and third parties*: The independent (e.g. from the business unit and risk management function) assessment of the firm's risk framework plays a crucial role in the ongoing maintenance of a firm's internal control, risk management and risk governance. It helps a firm accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. This may include internal processes, such as internal audit, or external processes such as third party reviews (e.g. external auditors, consultants).

FSB member jurisdictions are requested to provide a consolidated national response to the questionnaire, which should include descriptions of differences where these exist in oversight of risk governance within the jurisdiction (e.g. for banks vs. broker dealers, based on the size, business model, complexity of the firm), with a particular emphasis on any framework or behavioural changes that have occurred since the crisis. In order to limit the burden on FSB members and to avoid unnecessary duplication of information collection efforts, authorities can attach links to relevant documents (where available in English).

Feedback should be submitted by 11 May 2012 to fsb@bis.org under the subject heading "FSB Thematic Peer Review on Risk Governance." Individual submissions will not be made public.

---

[3] Risk appetite is the level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders. Risk appetite is generally expressed through both quantitative and qualitative means and should consider extreme conditions, events and outcomes. In addition, risk appetite should reflect potential impact on earnings, capital and funding/liquidity (see SSG report *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure*).

1. National authorities' approach toward risk governance oversight

1.1. Please describe your jurisdiction's overall approach to assessing firms' risk governance frameworks (e.g. legislation, regulation or supervisory guidance)? Please provide links to relevant documents. Has your jurisdiction evaluated whether such guidance is consistent with the BCBS or OECD principles on corporate governance or other recommendations provided by the industry?

1.2. How does your jurisdiction assess alignment or implementation of any legislation, regulation or supervisory guidance in the area of risk governance? How does your jurisdiction determine that your significant financial institutions have effective risk governance frameworks, policies and practices?

1.3. Please briefly describe whether firms in your jurisdiction have made changes in response to increased supervisory and regulatory oversight of risk governance. In addition, please provide examples of any material changes in the effectiveness of firms' risk governance practices over the last few years (e.g. decisions regarding whether to reduce/increase certain business activities based on the Board's risk strategy).

1.4. During the global financial crisis, were there weaknesses in your oversight of risk governance that became apparent? Please summarise any initiatives planned to strengthen your jurisdiction's oversight of firms' risk governance practices.

1.5. Does your jurisdiction regularly review whether your supervisory, regulatory and enforcement authorities are sufficiently resourced, independent and empowered to deal with risk governance weaknesses that have been identified? Does this review include an assessment of inter-agency as well as internal communication and decision-making processes?

1.6. Does your jurisdiction have dedicated teams of qualified personnel to assess firms' risk governance frameworks, or is oversight of risk governance embedded within other risk oversight functions (e.g. operational, market or credit risk)?

1.7. What regulatory and supervisory tools are available in your jurisdiction to incentivise firms to remediate deficiencies within the risk governance framework (e.g. restrictions on activities, capital charges, fines)? Please describe any regulatory or supervisory actions taken to incentivise firms to remediate weaknesses and the firm's responses (if possible in a way that respects national confidentiality rules).

1.8. How are relevant internal control weaknesses and other significant internal control deficiencies factored into the assessment of risk governance frameworks (e.g. a control deficiency that allows significant unauthorised trading activities)?

1.9. Please describe any bilateral efforts initiated by supervisors in other jurisdictions regarding the supervision of risk management policies and practices. Please indicate instances where supervisory work plans have been impacted as a result of those meetings.

2. Board responsibilities and practices

Risk committee[4] *refers to a specialised Board committee responsible for advising the Board on the firm's overall current and future risk appetite and strategy, and for overseeing senior management's implementation of that strategy. Risk committees comprising management members that reside below the Board level (e.g. within business units, management committees) do not fall in this definition.*

2.1. Do supervisory requirements or expectations exist concerning the role and responsibilities of the Board for risk governance? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)? Please provide your response in Table 1 of Annex A.

2.2. Do supervisory requirements or expectations exist concerning the role and responsibilities of the risk committee? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)? Please provide your response in Table 2 of Annex B.

2.3. Do supervisory requirements or expectations exist concerning the governance of the Board's own practices (and where they exist, the practices of any relevant sub-committees)? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)? Please provide your response in Table 3 of Annex C.

2.4. Do supervisory requirements or expectations exist concerning the information that Boards (or any relevant sub-committees) are supposed to receive, or able to request, from the firm (e.g. CRO, risk management function) and/or third parties (e.g. external auditors, consultants)? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)? Please provide your response in Table 4 of Annex D.

2.5. How does your jurisdiction assess whether supervisory expectations or requirements concerning the Board's responsibilities and practices (including the Board's use of sub-committees) are achieving desired outcomes?

[4] Where a self-standing risk committee does not exist, please answer the remaining questions in this questionnaire as per the arrangements applying for the full/members of the Board or the Board-level committee/s where the relevant risk responsibilities are allocated.

3. Risk management function

3.1. Does your jurisdiction require firms to have an independent senior executive (e.g. a Chief Risk Officer or equivalent) with distinct responsibility for the risk management function and the firm's comprehensive risk management framework across the entire organisation?

3.2. How does your jurisdiction assess the stature, authority and independence of the CRO (or equivalent) and the risk management function? Please outline what criteria are considered in your jurisdiction when assessing the stature, authority and independence. Please provide your response in Table 5 of Annex E.

3.3. How does your jurisdiction evaluate the qualifications of the CRO and risk management personnel? How does your jurisdiction evaluate the hiring and performance evaluation process of the CRO?

3.4. What is your jurisdiction's approach to regularly assessing firms' overall risk management policies and practices? Please provide your response in the Table 6 of Annex F.

3.5. How does your jurisdiction assess firms' implementation of effective risk appetite frameworks? Are risk measures clearly defined, actionable and effective in enabling the firm to pursue its strategic objectives and maintain the risk profile as set out in the risk appetite framework? Is the risk appetite assessed globally, or for each type of risk (e.g. credit, market, liquidity, operational)?

3.6. How does your jurisdiction regularly assess the adequacy of firms' risk management resources (e.g. number, quality, effectiveness)?

3.7. Does your jurisdiction review the "ownership" and accountability of risk management resources?

3.8. How does your jurisdiction assess the role and effectiveness of firms' risk management process for (i) approval of new products and material modifications to existing ones; (ii) strategic planning; (iii) changes in systems, processes, business models; and (iv) major acquisitions?

3.9. What work has been undertaken in your jurisdiction to assess the adequacy, timeliness, and independence of information prepared by risk management and provided to senior management and the Board (or any relevant sub-committee)?

3.10. How does your jurisdiction evaluate the type and nature of risk reporting to the Board (or any relevant sub-committee)? Does it include (i) the manner in which information is compiled; (ii) what the decision-making process is for information to be included in the Board reporting; and (iii) who/what part of the firm is responsible for compiling this material?

3.11. Does your jurisdiction collect standardised information from firms on certain risk areas to (i) compare firms' across risk dimensions; (ii) identify the need to initiate possible supervisory reviews; or (iii) update supervisory risk management expectations?

3.12. Does your jurisdiction assess the effectiveness of firms' forward-looking stress tests, scenario analysis, contingency arrangements, recovery plans (e.g. raising capital or reducing exposures) and resolution plans (if any). If so, what criteria are used in this assessment?

3.13. How does your jurisdiction incorporate market and macroeconomic conditions, cross-sectoral developments as well as changes in firms' business and risk profile into your evaluation of the adequacy of risk management and its ability to respond to changing circumstances? To what extent are the requirements for the risk management function adapted to firm characteristics, such as size, complexity, business model and systemic importance?

4. Assessment of the risk governance framework

4.1. Does your jurisdiction require internal audit functions at firms to assess the firm's risk governance framework at the enterprise level, legal entity level, and/or for the largest revenue-generating business units? If so, are the requirements specified in legislation, regulation or supervisory guidance? Please provide your response in Table 7 of Annex G.

4.2. What aspects of the risk governance framework are internal auditors or other internal functions (if independent) expected to assess?[5] Are supervisory requirements and expectations specified in legislation, regulation or supervisory guidance? Please provide your response in Table 8 in Annex H.

4.3. Does your jurisdiction allow the use of third parties (e.g. external auditors or other experts) to provide an independent assessment of firms' risk governance frameworks? If so, does your jurisdiction impose any limitations on certain aspects of internal audit's responsibilities that can be directed toward third parties (e.g. outsourced)? Are supervisory requirements and expectations specified in legislation, regulation or supervisory guidance? Please provide your response in Table 9 of Annex I.

4.4. What aspects of the risk governance framework are external experts expected to assess? Are supervisory requirements and expectations specified in legislation, regulation or supervisory guidance? Please provide your response in Table 10 of Annex J.

---

[5] The independent assessment of a firm's risk governance framework is often performed by internal audit, but in some firms there may be other internal functions that contribute to the assessment. In cases where these "other internal functions" are considered to be sufficiently independent, the expectations associated with these functions should be included in your responses to questions about internal audit.

4.5. Are internal audit reports, prudential reports, and/or external expert reports monitored as part of the supervision of a firm's risk governance assessment process? If so, please describe the types of reports and frequency of review.

4.6. How does your jurisdiction evaluate the qualifications of the internal auditor and internal audit personnel? How does it evaluate the hiring and performance evaluation process of the chief auditor (or equivalent)? Where relevant, is this evaluation process also applied to third parties (as defined in 4.3)?

4.7. How does your jurisdiction conduct assessments of the governance of firms' risk management at the enterprise level (e.g. through on-site inspections, off-site monitoring, standard reporting mechanisms, supervisory colleges)?

4.8. Are escalation processes in place to facilitate the communication of specific situations/behaviours by individuals within a firm to the supervisor (escalation process and/or whistle-blowing)?

4.9. Does your jurisdiction monitor firms' remediation of weaknesses identified by the independent assessment of risk governance functions? If so, is the monitoring embedded in the supervisory process or based on firms' progress reports?

Annex A

Please provide your answer to question 2.1 in Table 1 below.

Question 2.1: Do supervisory requirements or expectations exist concerning the role and responsibilities of the Board for risk governance? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)?

Table 1: Role and responsibilities of the Board		
Do supervisory requirements or expectations concerning Board responsibilities cover:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
a) risk governance, including approval of the firm's risk strategy (e.g. risk tolerance, risk appetite, business strategy)?		
b) oversight of senior management's implementation of the firm's risk strategy?		
c) approving and overseeing the implementation of the firm's policies for risk, risk management and compliance relating to risk management?		
d) approving and overseeing the implementation of the firm's internal controls system relating to risk management?		
e) the responsibilities to explicitly formulate and define how they assume the responsibilities relating to risk management?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 1: Role and responsibilities of the Board		
Do supervisory requirements or expectations concerning Board responsibilities cover:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
f) communication with national authorities, including requirements for meetings between the Board and supervisors on risk governance issues?		
g) in a group structure, overall risk governance responsibilities across the group and for the group as a whole?		

Annex B

Please provide your response to question 2.2 in Table 2 below.

Question 2.2: Do supervisory requirements or expectations exist concerning the role and responsibilities of the risk committee? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)?

Table 2: Role and responsibilities of the risk committee		
Is it required or expected that:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
a) the risk committee be a self-standing committee[6], or can its functions and responsibilities be shared across several Board committees?		
b) the role and responsibilities of the risk committee is to advise the Board on the firm's overall current and future risk tolerance/appetite and strategy?		
c) the risk strategies 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?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

6 Where a self-standing risk committee does not exist, please answer the remaining questions in this questionnaire as per the arrangements applying for the full/members of the Board or the Board-level committee/s where the relevant risk responsibilities are allocated.

Table 2: Role and responsibilities of the risk committee		
Is it required or expected that:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
d) the role and responsibilities of the risk committee is to oversee senior management's implementation of the risk strategies, making operative the Board-approved risk tolerance/appetite?		
e) in a group structure, the risk committee's mandate should take into account the group structure that the firm operates in?		
f) risk committees discuss 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)		

Annex C

Please provide your response to question 2.3 in Table 3 below.

Question 2.3: Do supervisory requirements or expectations exist for the governance of the Board's own practices (and, where they exist, the practices of any relevant sub-committees)? If so, how have these expectations been established (e.g. legislation, regulation, supervisory guidance)?

Table 3: Governance of the Board and risk committee		
Do supervisory requirements or expectations for governance of the Board and risk committee cover:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
a) that the composition of the Board and risk committee include a minimum proportion of independent members, and there is a clear definition of independent member (if so, please define)?		
b) that members of the Board and risk committee meet certain qualifications, including passing fit and proper tests and possess certain skills (e.g. technical financial understanding in risk disciplines, business experience in risk issues)?		
c) limits on involvement/ participation by the Chair of the Board in the risk committees (e.g. the Chair of the risk committee cannot be the Chair of the Board)?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 3: Governance of the Board and risk committee		
Do supervisory requirements or expectations for governance of the Board and risk committee cover:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
d) that qualifications of the members, the skill set across the Board and risk committee, and the benefits of renewal be taken into account in selecting members?		
e) procedures for reporting from the risk committee to the Board and from the Board to risk committee?		
f) routines for co-ordination and communication among different Board sub-committees that deal with issues relevant for overall risk assessments?		
g) a periodical review of the performance, training and skills needed in the Board and risk committee?		
h) a periodical review of the functioning of the overall committee structure used by the Board?		

Annex D

Please provide your response to question 2.4 in Table 4 below.

Question 2.4: Do supervisory requirements or expectations exist concerning the information that Boards (or any relevant sub-committees) are supposed to receive, or able to request, from the firm (e.g., CRO, risk management function) and/or third parties (e.g. external auditors, consultants)? If so, how have these requirements or expectations been established (e.g. legislation, regulation, supervisory guidance)?

Table 4: Information provided to the Board and its sub-committees		
Is it expected or required that:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
a) the Board/risk committee is able to receive information, both formally and informally, from either the CRO or the risk management function?		
b) the Board/risk committee can communicate and meet with the CRO?		
c) the information received by the Board/risk committee is in a standard form, frequency and contains certain minimum information?		
d) the Board/risk committee receives information on only the overall risk level of the firm, or detailed information for each type of risk and each business unit?		
e) procedures for communication among Board-level committees dealing with risk assessments as well as their mandates and responsibilities are defined by the Board?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 4: Information provided to the Board and its sub-committees		
Is it expected or required that:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
f) an independent model validation unit exists and reports to the risk committee and other relevant bodies?		
g) the Board/risk committee can have access to external expert advice?		

Annex E

Please provide your response to question 3.2 in Table 5 below.

Question 3.2: How does your jurisdiction assess the stature, authority and independence of the CRO (or equivalent) and the risk management function? Please outline what criteria are considered in your jurisdiction when assessing the stature, authority and independence.

Table 5: Stature, authority and independence of the CRO (or equivalent) and the risk management function	
Are the CRO (or equivalent) and the risk management function expected to:	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
a) have a distinct role from other executive functions, revenue-generating functions and business line responsibilities, and there generally is no "dual hatting" (the chief operating officer, chief financial officer, chief auditor or other senior management should not also serve as the CRO)?	
b) report and have direct access to the Board and its sub-committees without impediment?	
c) interact with the Board regularly and these interactions be recorded adequately?	
d) be able to meet with non-executive Board members in the absence of senior management?	
e) have the ability to influence decisions that affect the firm's exposure to risk?	

Table 5: Stature, authority and independence of the CRO (or equivalent) and the risk management function	
Are the CRO (or equivalent) and the risk management function expected to:	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
f) have access to information and to all relevant affiliates / subsidiaries?	

Annex F

Please provide your response to question 3.4 in Table 6 below.

Question 3.4: What is your jurisdiction's approach to regularly assessing firms' overall risk management policies and practices?

Table 6: National authorities' approach to assessing firms' risk management framework	
Please describe the:	**Please briefly describe the approach for assessing overall risk management policies and practices and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.**
a) frequency of evaluations conducted	
b) types of reports or information collected from firms on their risk management practices	
c) types of reports or information collected on firms' risk management practices from third parties (e.g. external auditors, consultants)	
d) seniority of individuals you meet with at the firm (e.g. Board members, CRO, CRO direct reports, risk managers with oversight responsibilities)	

Annex G

Please provide your response to question 4.1 in Table 7 below.

Question 4.1: Does your jurisdiction require internal audit functions at firms to assess the firm's risk governance framework at the enterprise level, legal entity level, and/or for the largest revenue-generating business units? If so, are the requirements specified in legislation, regulation or supervisory guidance?

Table 7: Role and responsibilities of internal audit		
Are internal audit functions expected to:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
a) be a permanent function at firms?		
b) be independent from risk management functions (e.g. compliance, permanent control, model validation functions)?		
c) report directly to the Board from an organizational perspective and with regards to findings?		
d) conduct assessment and testing functions at a specified frequency (e.g. quarterly, semi-annually, annually)?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 7: Role and responsibilities of internal audit		
Are internal audit functions expected to:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
e) in the case of specifically complex financial structures, conduct internal audits at various firm levels to assess the firm's overall structure and individual entities' activities and confirm compliance with the overall strategy previously approved by the Board?		
f) confirm compliance with the firm's risk profile as approved by the Board?		
g) have a process for monitoring the remediation of material deficiencies identified, i.e. assess the follow up of internal audit's recommendations?		
h) see its independence ensured through compensation or career plans?		
i) use formalised tools during the auditing process (procedures, audit guides, audit charter, etc.)?		

Annex H

Please provide your response to question 4.2 in Table 8 below.

Question 4.2: What aspects of the risk governance framework are internal auditors or other internal functions (if independent) expected to assess? Are supervisory requirements and expectations specified in legislation, regulation or supervisory guidance?

Table 8: Independent assessments by internal audit		
Does the scope of work include opinions and/or assessments of:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
a) the organisation and mandates of the risk management functions including market, credit, liquidity, interest rate, operational, and legal risks?		
b) the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting all the firm's risks due to business activities?		
c) management's risk assessments, policies, risk limits, controls, and operating procedures?		
d) the appropriateness of assumptions used in scenario analysis and stress testing?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 8: Independent assessments by internal audit		
Does the scope of work include opinions and/or assessments of:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
e) the consistency, timeliness, independence, and reliability of data sources used in such models?		
f) the degree to which the firm's risk governance is keeping pace with industry trends and aligns with best practices?		
g) the quality and adequacy of resources within the risk management function?		
h) the overall efficiency and integrity of risk management information systems, including the accuracy, reliability, and completeness of the data used?		
i) the effectiveness of the risk and issue escalation and resolution process?		

Annex I

Please provide your response to question 4.3 in Table 9 below.

Question 4.3: Does your jurisdiction allow the use of third parties (e.g. external auditors or other experts) to provide an independent assessment of firms' risk governance frameworks? If so, does your jurisdiction impose any limitations on certain aspects of internal audit's responsibilities that can be directed toward third parties (e.g. outsourced)? Are supervisory requirements and expectations specified in legislation, regulation or supervisory guidance?

Table 9: Role and responsibilities of third parties		
Where third parties have a role in assessing firms' risk governance frameworks, are they expected to:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
a) report findings directly to the Board?		
b) avoid conflicts of interest with the business unit being audited (i.e. the hiring of third-parties and their compensation is not conducted by the business unit being audited)?		
c) conduct assessments at a specified frequency?		
d) in the case of specifically complex financial structures, conduct assessments at various firm levels of the firm's overall structure and individual entities' activities and confirm compliance with the overall strategy previously approved by the Board?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 9: Role and responsibilities of third parties		
Where third parties have a role in assessing firms' risk governance frameworks, are they expected to:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
e) confirm compliance with the firm's risk profile as approved by the Board?		
f) assess the resolution of material deficiencies identified by the independent assessment function, i.e. assess the follow up of internal or external audit's recommendations?		
g) use formalised tools during the auditing process (procedures, audit guides, audit charter, etc.)?		

Annex J

Please provide your response to question 4.4 in Table 10 below.

Question 4.4: What aspects of the risk governance framework are external experts expected to assess? Are supervisory requirements and expectations specified in legislation, regulation or supervisory guidance?

Table 10: Independent assessments by third parties		
Does the scope of work include opinions and/or assessments of:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance.** **Please provide links to internet sites.**
a) the organisation and mandates of the risk management functions including market, credit, liquidity, interest rate, operational and legal risks?		
b) the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting all the firm's risks due to business activities?		
c) management's risk assessments, policies, risk limits, controls, and operating procedures?		
d) the appropriateness of assumptions used in scenario analysis and stress testing?		

* L = Legislative R = Regulatory S = Supervisory Guidance O = Other

Table 10: Independent assessments by third parties		
Does the scope of work include opinions and/or assessments of:	**Approach L/R/S/O***	**Please briefly describe the requirement or expectation and explain any differences (i) for banks vs. broker-dealers, or (ii) based on a firm's size, business model, complexity and systemic importance. Please provide links to internet sites.**
e) the consistency, timeliness, independence, and reliability of data sources used in such models ?		
f) the degree to which the firm's risk governance is keeping pace with industry trends and aligns with best practices,?		
g) the quality and adequacy of resources within the risk management function?		
h) the overall efficiency and integrity of risk management information systems, including the accuracy, reliability, and completeness of the data used?		
i) the effectiveness of the risk and issue escalation and resolution process?		