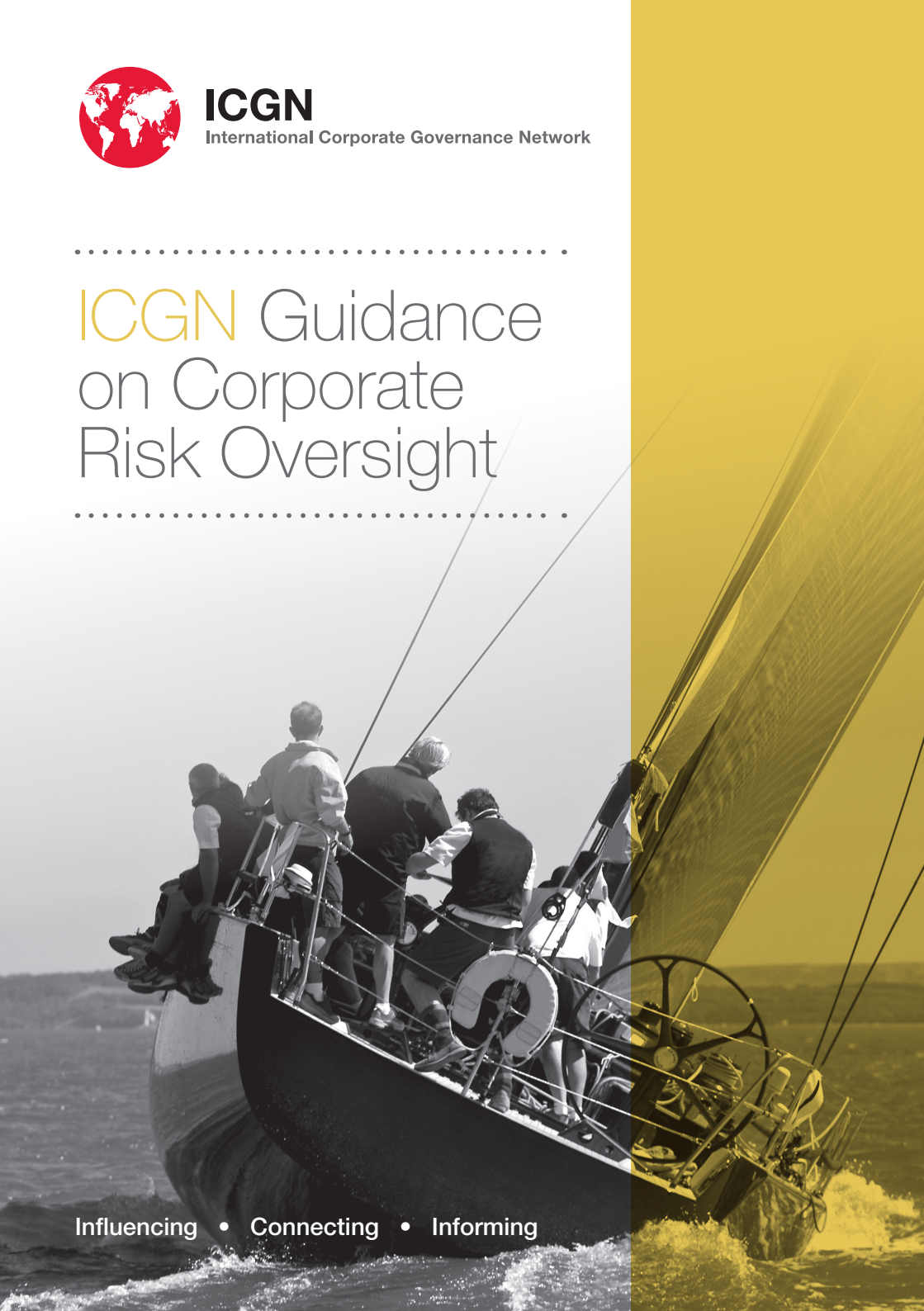
ICGN
International Corporate Governance Network

ICGN Guidance on Corporate Risk Oversight



Influencing • Connecting • Informing

Published by the International Corporate Governance Network 2015. 3rd Edition.

British Library Cataloguing in Publication Data
ISBN 978-1-907387-13-5

ICGN Guidance on Corporate Risk Oversight

Preamble

The International Corporate Governance Network (ICGN) is an investor-led body with a mission to inspire and promote good governance standards to advance efficient markets worldwide. Established in 1995 and present in over 45 countries the ICGN membership includes global investors with assets under management in excess of US$ 26 trillion. ICGN Principles and Guidance are therefore substantively developed from an investor perspective, while taking into account other parties including companies, professional advisors and academics.

For companies and investors alike, risk taking is an inseparable element of strategy and a crucial driver in achieving objectives, including optimising value over time. Risk is part of every decision a company makes. Strategy and risk are not new concepts, although it is recognised that risk is a subject of increasing attention and regulatory and legislative movements in many jurisdictions. The board's and investors' ability to gauge and respond to how a company understands and manages risk has broader relevance beyond the board and investors alone. It bears on the company's impact on all stakeholders including employees and the communities in which a company does business, and in certain instances, national or international markets.

Financial stability and non-financial factors are both important determinants of corporate strategy. Risk and risk oversight must therefore be understood broadly. In this document risk is defined[1] as the effect of uncertainties on corporate objectives, recognising that the effect can be either positive or negative. Boards and investors need to consider material risks which are manageable within the organisation's sphere of influence including but not limited to financial, market, operational, environmental, ethical, fraud, legal and compliance, reputational, environmental and social risks. Risk oversight is defined as the board's supervision of the risk management framework[2] and risk management process[3]. Risk management, as a responsibility of a company's management team, is distinct from risk oversight.

Boards and investors have a joint responsibility to engage in substantive and effective communication on corporate risk oversight. Communication models and methods for this should not be any different than for other corporate governance matters. However, the topic of corporate risk oversight is a subject on which boards and investors should engage. Active, informed, constructive and periodic communication between board members and investors is crucial for a mutual understanding of corporate strategy, risk and risk oversight. Such dialogue should be founded upon an appropriate and comparable level of respect, trust, seniority, skill and professionalism between investors and companies.

The objective of this guidance is to help investors assess how well a portfolio company's board either[4] is effectively overseeing risk management. Further, the targeted audience is broader than just company boards and investors; it includes auditors, risk advisory and rating firms as well as provincial, national and international supervisory bodies.

This Guidance assumes the following about the design of risk governance, including process, roles and measurement of outcomes:

- The risk oversight process begins with the board. The unitary or supervisory board has an overarching responsibility for deciding the company's strategy and business model and understanding and agreeing on the level of risk that goes with it. The board has the task of overseeing management's implementation of strategic and operational risk management.

- Corporate management is responsible for developing and executing a company's strategic and routine operational risk programme, in line with the strategy set by the board and subject to its oversight.

- Shareholders, directly or through designated agents, have a responsibility to assess and monitor the effectiveness of boards in overseeing risk at the companies in which they invest and to determine what level of resources they will dedicate to this task. Investors are not themselves responsible for risk oversight at corporations.

This Guidance specifically address the challenges investors have, directly or through agents, in addressing risk at specific portfolio companies. However, it is well-recognised that investors also need to address risks in other ways that lie beyond the scope of this guidance. For instance, they should identify, understand and take responsibility for how risks are managed in indexed portfolios. They should understand and take steps to manage their exposure to portfolio risks that could result from aggregation of investments which are exposed to similar events. In any case, beneficial owners should monitor and make conscious choices involving risk based on an evaluation of long-term effects on the interests of underlying fund beneficiaries and participants.

The Guidance does not in any way seek to eliminate or minimise risk taking. In a healthy dynamic market profits are largely sourced from risk taking. Companies and investors alike are aware of this. However, a sound risk management programme should demonstrably identify and reduce the frequency of potentially large loss events. Such large loss events may be particularly likely to occur as a result of a failure to manage portfolio risk, rather than as the result of the company-specific risk.

The Guidance is divided into four sections. Part 1 clarifies the ICGN principles on corporate risk oversight; Part 2 follows with guidance on the board process related to corporate risk oversight. Part 3 follows with guidance on disclosure relating to corporate risk. Part 4 focuses on example questions for the dialogue between companies and investors.

The ICGN Corporate Risk Oversight Guidance is intended to be of general application globally, while recognising that companies are obliged to comply with applicable national legislative frameworks, regulatory disclosure requirements or listing rules. As global guidance, it should be read with an understanding that local rules and cultural norms may lead to different approaches to governance practices. ICGN Members support the flexible application of this Guidance and therefore the specific circumstances of individual companies, investors and the markets within which they operate should be recognised. The Guidance supplement the ICGN Global Governance Principles which clarify the responsibilities of boards of directors and investors in their mutual interest to protect and generate corporate value over the long term.

Contents

Part 1: ICGN Principles on corporate risk oversight

The ICGN Global Governance Principles define the following in terms of corporate risk oversight:

Proactive oversight

The board should proactively oversee, review and approve the approach to risk management regularly or with any significant business change and satisfy itself that the approach is functioning effectively. Strategy and risk are inseparable and should permeate all board discussions and, as such, the board should consider a range of plausible outcomes that could result from its decision-making and actions needed to manage those outcomes.

Comprehensive approach

The board should adopt a comprehensive approach to the oversight of risk which includes all material aspects of risk including financial, strategic, operational, environmental, and social risks (including political and legal ramifications of such risks), as well as any reputational consequences.

Risk culture

The board should lead by example and foster an effective risk culture that encourages openness and constructive challenge of judgements and assumptions. The company's culture with regard to risk and the process by which issues are escalated and de-escalated within the company should be evaluated at intervals as appropriate to the situation.

Dynamic process

The board should ensure that risk is appropriately reflected in the company's strategy and capital allocation. Risk should be managed accordingly in a rational, appropriately independent, dynamic and forward-looking way. This process of managing risks should be continual and include consideration of a range of plausible impacts.

Risk Committee positioning

While ultimate responsibility for a company's risk management approach rests with the full board, having a risk committee (be it a stand-alone risk committee, a combined risk committee with nomination and governance, strategy, audit or other) can be an effective mechanism to bring the transparency, focus and independent judgement needed to oversee the company's risk management approach.

Part 2: Guidance on board process

2.1 Proactive risk oversight

The corporate board has a responsibility to take steps to ensure that it has a proactive and dynamic approach that results in effective oversight of risk management.[5]

Strategy, risk and risk management are inseparable and should be connected in all discussions by the board or supervisory board. Capital allocation and capital structure should be visibly aligned with strategy and risk appetite. The board should hold management accountable for developing a strategy that correlates with the risk appetite of the organisation.

Boards are responsible for approving corporate strategy and overseeing enterprise risk management, including risk appetite. These should be connected to an appropriate risk management methodology based on an established risk management process. The board should hold management accountable for designing and implementing a risk management system. The risk management framework, allocated staff and resources should be appropriate and sufficient to properly conduct the risk management process.

2.2 Comprehensive approach

A common definition of risk must be understood by all stakeholders within an organisation. The critical aspect of the definition is that the board, management and employees understand the meaning of risk as it relates to their individual responsibilities.

Boards should ensure that management has a company-wide view of risk which contemplates the potential effects of simultaneous interaction among the various risks, both on the company and the wider financial system. Such an aggregated view should be evaluated at least annually for alignment with the organisation's strategic plan and objectives and regularly reported to the board.

2.3 Risk culture

Board dynamics are fundamental to the decision making process for overseeing strategy and risk management. Non-executive board members have an important role and should have the ability to improve or challenge boardroom dynamics. It is the responsibility of all board members to exercise independent and active oversight. It is crucial that independent judgement be supported by a far reaching understanding of the company, its strategy, and its industry. Boards should lead by example and foster an effective and demanding risk culture in the boardroom and the broader company. Boards should specify their expectations of a risk culture for the enterprise.

A company's culture and organisational structures should encourage openness, dynamic dialogue on risk and strategy, as well as constructive challenge of judgment and assumptions. Periodic assessments should be undertaken to evaluate both the company's and the board's culture with particular regard to risk and the process by which issues are escalated and de-escalated within the company.

2.4 Dynamic process

Boards are responsible for overseeing the way in which the risk management process recognises, prioritises and effectively responds to risk. Boards should maintain an active and alert attitude to unforeseen risk. They should be attentive not just in the context of negative events, but also by taking onto account the changing landscape of opportunities and threats. They should also understand stakeholder opinions and impacts that could alter the effectiveness of a company's strategy or even the viability of a company and or its industry. Boards should be particularly mindful of systemic risks, where risk taking behaviour by one or more companies can compound to the detriment of the company's investors, other stakeholders, and even society more broadly.

2.5 Risk Committee positioning

Responsibility for risk oversight rests with the full board, even if a risk committee or other specialised committees are established. Delegation of responsibility to specialised committees is an important tool in strengthening the board's capacity in overseeing risk. If the board allocates responsibility for risk oversight to one or more committees, it should describe the terms of reference for these bodies in its corporate governance principles and committee charters and ensure that members have sufficient skills in strategy, operations and understanding of the company. The board should determine how the work of its committees is to be coordinated and how it is integrated in the board's discussions on strategy.

Boards should directly influence the risk profile of a company. This includes making key decisions such as setting boundaries outside which the management is not permitted to operate; defining succession plans for top management; defining a selection process for new members of the board and of top management; and defining incentive schemes for top management.

2.6 Non-executive board members

Non-executive board members, through a specialised committee, and/or the outside chair or lead or senior independent director, should collaborate with executive directors and management to determine which information the non-executive board members receive on risk matters -- and how frequently.

Non-executive board members should have the rights and capacity to obtain information from other sources and advisors, including those outside the company. Clarity in decision making structures and a disciplined approach to risk taking should not preclude boards from actively gathering additional information from any member of executive management.

2.7 Board competency

In order for the board to be equipped to carry out its responsibility for risk oversight, it must have a sufficient knowledge and understanding of the company and its industry. Boards should assure themselves through periodic assessments that the board composition and director skill sets are appropriate for effectively overseeing the process and content of material risk. Gaps in necessary collective competencies or knowledge can be addressed by educational programmes and through the selection process for new board members. Whatever body is charged with selecting director candidates, it should ensure that nominees have the appropriate level of capability and related experience commensurate with the strategic and risk complexity of the company.

2.8 Access to information

Reliable and timely information are important features as they allow boards to incorporate insightful information in making decisions. Information protocols within a company should allow for and anticipate the continually changing landscape in which companies operate. The board must recognise that a failure to act on information it has can be just as damaging as not having the information at all.

Boards should determine that the risk information provided to the board is complete and reliable with regard to identified risks and that the management has undertaken all reasonable endeavours to identify all material risks. Boards should periodically pose the question as to whether or not current management has the capacity to effectively identify, explain and execute strategy and risk processes. Boards should ensure that such responsibilities and skills are among job performance benchmarks for senior executives both as part of succession planning, ongoing supervision of management and executive remuneration policies.

2.9 Chief Risk Officer

The board should determine if it is appropriate for the company to create a dedicated management position responsible for risk identification and reporting to the board for example, a chief risk officer (CRO). The board should establish, and publicly communicate, the criteria that underpin such a decision.

If the board determines that such a dedicated position is not necessary, then

it should identify the person or persons who are to assume responsibilities for risk management, commensurate with the role of a chief risk officer. An executive, like the Chief Financial Officer, where the role includes the responsibilities of the CRO. The executive has access but does not report to the non-executive directors of the Risk Committee or the committee with the responsibility to oversee risk.

If the board determines that such a dedicated position is necessary, then a dedicated CRO should report directly, and independently of executive management, to the Risk Committee. The position of a chief risk officer or equivalent should be empowered by the requirement that only independent directors - and not executive management - can alter the terms of employment.

2.10 Dialogue with investors

Boards should make available to investors one or more communication channel(s) for periodic dialogue on governance matters, including the board's role in risk oversight. Boards should clearly explain such procedures to investors, including guidance related to compliance with fair disclosure and other relevant market rules. Boards should regularly invite investors to express views and concerns regarding strategy and risk oversight.

2.11 Investor responsibility

Investors should take effective steps to assess a board's oversight of risk with respect to the company's strategy.

In carrying out ownership responsibilities, it is incumbent upon investors to have the capacity to inform themselves of and monitor on an ongoing basis, the quality of strategy and risk oversight by boards of investee companies. They may do so by relying on company disclosures, in-house research and/or external sources.

2.12 Investor self-assessment

Investors should, on a periodic basis, undertake an assessment of their own resources, skill base and outsourcing options to ensure that they meet agreed levels of responsibility for monitoring boards on risk oversight. The assessment could include, for example, a review of whether and how internal remuneration, job descriptions and staff performance reviews may be tied in part to such analyses. Investors should provide beneficiaries with a periodic statement explaining their strategy and capacity for analysing and monitoring current or prospective portfolio companies for strategy, risk oversight, and risk management. For example, where they utilise external services for this, they should consider disclosing the name of the provider of the services in question, the nature of the mandate they have been given and procedures for monitoring performance of the provider. The external provider should be asked by the investor to provide regular updates on how they fulfil this aspect of their mandate.

Part 3: Guidance on disclosure

3.1 Comprehensive information

The board should concisely disclose information sufficient for investors to make judgments on the quality of the board's oversight of the risk management process.

The periodic risk oversight statement to investors, should include information on at least the following:

- how and how often strategy, level of risk appetite, and risk oversight are assessed by the board in connection to each other;
- how and how often the suitability of the capital structure, the capital allocation process, the risk management framework and the risk management system are assessed with respect to strategy and risk appetite;
- how and how often the structure of information flow and levels of decision making regarding actively taken risks are assessed with regard to effective risk oversight;
- how and how often stakeholders are considered in the risk management process;
- how the board addresses its responsibility for risk oversight in its annual evaluation process.

3.2 Frequency

Disclosure should be made at least annually, in conjunction with an organisation's regular financial reporting process.

3.3 Format

Boards should provide investors with a statement that includes information on risk oversight procedures and board perspectives on risk in the approved strategy. This should be in a text identified as distinct from any reports or disclosures issued by management concerning specific risks faced by the company. The disclosure statement should be consistent with the size and complexity of the company.

3.4 Structure

Boards should explain to investors those aspects of the corporate governance structure that the board relies upon to oversee the strategy and material risks of the company, including whether a board level committee specialised in risk exists, the nature of its responsibilities, skills and the feedback loop into the board's strategy discussions.

3.5 Policy

In disclosures, a board should describe the company's approach to risk within the context of current corporate strategy, the process used to set parameters of the company's risk tolerance, the frequency with which these parameters are reviewed, and whether any limits on risk-taking are imposed on management.

Boards should disclose (any changes in) material risks, including changes that result from modifications of strategy as well as changes in the company's environment (e.g., market shares and competitors).

Boards should disclose how they monitor the robustness of contingency and resilience planning for risk threats and opportunities.

Boards should clearly articulate how they ensure that variable pay practices for executives align with the company's strategy and risk management and the current state of the company.

3.6 Process

Boards should explain to investors it has collectively reviewed, challenged and approved management's information on company risk and risk management in light of the company's strategy.

Boards should disclose risk oversight challenges that may have emerged over the reporting period, including actions taken or plans to address them. The board should describe how it dealt in respect of procedure with any failures of risk oversight. The board should explain how on an ongoing basis it seeks to improve risk oversight

Boards should disclose how they ensure that broader economic risks and systemic industry risk that can affect probabilities of achieving the company objectives are taken into account. This explanation should include consideration of multiple events occurring simultaneously.

3.7 Board competency

Boards should provide sufficient information on their own members so that investors can effectively evaluate the full board's integrity and qualifications. For instance, boards may disclose member competencies, continuing education programmes, industry and risk management knowledge and experience, and adherence to board ethics standards. Boards are encouraged to communicate openly about any current identified gaps in board competence and their course of action to address these.

Part 4: Company and investor dialogue

Information on risk

1. What are the material risks that the company faces, in the context of the organisational strategy and its industry sector?
2. How much risk is the company taking in order to achieve its strategic objectives?
3. Does the management maintain an adequate risk management system?
4. Does the board possess the competencies, structures and processes to maintain risk oversight?

Proactive risk oversight

5. Does the board have a framework to make meaningful judgments about risk tolerance and risk appetite?
6. How does the board assess whether it understands its mandate and role in risk oversight?
7. Does the board periodically consider and quantify the corporation's capability to take on and manage risk?
8. In which areas of the company is risk policy most challenged?
9. How does the company define and disclose its material strategic risks?
10. What business environment risks might be created by the actions of the company and its industry?
11. Can the board explain the risk considerations that underpin any changes in strategy?
12. Does the company have a crisis management plan in place?

Comprehensive approach

13. How does the board assess whether there is an effective and comprehensive risk management system in place?
14. What evidence is there that the board and management are aligned in their view of the board's role in risk oversight?
15. How do members of the board familiarize themselves with trends or potential risks specific to the company?

Risk culture

16. What measures does the board take to instil from the top and throughout the company a culture of risk monitoring and accountability?
17. What steps does the board take to ensure that management at relevant levels of the company understands that the board maintains robust oversight of risk management?
18. What is the risk culture in the company? How does it compare to the desired risk culture in the company? How does the design of risk oversight and risk management support the desired risk culture?
19. Does the board maintain, monitor and refresh an ethics policy for itself and employees and, if so, how is such policy embedded throughout the organisation?
20. Can the board explain (irregular) changes in the composition of the board and management?

Structures

21. How does the board allocate risk oversight responsibilities between its committees?
22. How does the board ensure effective communication between its committees with respect to risk?
23. Can the company clearly define the relationship between the risk, audit, and remuneration committees? How does the board avoid committees working in isolation of each other?
24. To what extent does the board retain independent counsel and expertise in executive remuneration and CEO succession & selection to ensure effective organizational and leadership risk management?
25. In financial services firms, who is responsible for setting overall trading and or credit limits? How are individually-assigned limits or group limits associated with similar types of risk set, monitored and controlled?
26. How is it evaluated and decided as to whether a dedicated risk management function should be created?
27. What are the specific criteria of a company's risk management system on which the creation of a Corporate Risk Officer function is based?

Dynamic process

28. How many risk issues were communicated to the management and the board within the last year and what was their response to these issues?
29. Who are the company's most highly remunerated employees and why? Are their incentives based on risk-adjusted performance, and if so, how?
30. How effective is the company's whistle-blowing policy, and how often is it used?
31. How much board or management time is spent on contingency planning (i.e. resilience planning rather than identification of risks)?

32. What were the main recommendations relevant to risk management from the last board evaluation and what has been done to address them?

33. What were the main recommendations concerning risk made by the external auditor, and what has been done to address them?

34. Does the board have a clear picture of the risk related to the macro environment and geopolitical environment in which it is working?

35. Does the board have the necessary blend of business and industry knowledge and experience to assess risk?

36. How does the board assess the effectiveness of its risk management systems in enabling the business model to deliver sustainable profits?

37. Does the board have an adequate system of assurance in place to assist with the company's risk oversight responsibilities?

Access to information[6]

38. How does the board demonstrate that it has an adequate and up-to-date appreciation of the nature, types and sources of risk faced by the organization?

39. Does the board have access to unfiltered information from management about the risks facing the company?

Results

40. Can an executive describe the role of risk oversight in his or her daily job in association to the company's business and strategy?

41. What evidence demonstrates that the board, on an ongoing basis, is committed to improving risk oversight?

42. What is management doing to improve risk management? What were the latest improvements and which improvements are currently being worked upon?

Crisis management[7]

43. How does the board get information during a crisis?

44. How does the board determine its role in a crisis?

45. How does the organization determine how and what it will communicate with stakeholders following a crisis?

46. Does the board consider information from investors that may avert a crisis?

47. How effective are management and the board in identifying early warning signals?

48. What are the plans for business continuity following a crisis?

• *See opposite page for steps a board should consider in a crisis*

Crisis management

Crisis has struck: Immediate steps a board should take during a crisis

Required action	Why
Designate immediate spokesperson for the board	To take immediate charge of project stability, continuity and control over the situation.
Appoint crisis management team	To report directly to appropriate board committee. Crisis team should be unrelated to events that led to crisis
Appoint independent legal and/or forensic/ technical specialist	To conduct an internal investigation of events leading to crisis
Check if adequate governance mechanisms are in place	To ensure management and board succession plans are robust and ready for activation and to ensure appropriate disclosure mechanisms are in place.
Assess the role of the external auditors	To determine if the nature of the crisis relates to accounting standards, and if so, to which extent auditors had identified red flags and properly alerted the board; if appropriate, to take remedial measures.
Develop and implement communications plan	To keep key stakeholder including regulators, investors, customers and employees informed
Institute appropriate board governance mechanisms	To enable timely, frank, and where needed executive session-only, discussions

End Notes

[1] *This definition, as other definitions in this document, is in line with the definition as stated in the ISO Guide 73. Risk oversight is not a defined term in ISO guidelines.*

[2] *The risk management framework is defined in line with the ISO Guide 73 as the set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring (3.8.2.1), reviewing and continually improving risk management (2.1) throughout the organization. References between brackets refer to the ISO Guide 73.*

[3] *Risk management process is defined in line with the ISO Guide 73 as the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring (3.8.2.1) and reviewing risk (1.1). References between brackets refer to the ISO Guide 73.*

[4] *The principles are intended to apply to both a single-tier board and a two-tier board structure. When referring to the "full board" or "the board" it is intended that this be specific to the actions of the non-executive and other directors that may comprise the supervisory board in a two-tier system or the unitary board in a single-tier system.*

[5] *An example of further guidance and information is the Financial Reporting Council's Guidance on Risk Management, Internal Control, and related Financial and Business Reporting (2014).*

[6] *A Framework for Board Oversight of Enterprise Risk, John Caldwell CPA, CA, Chartered Professional Accountants of Canada, 2012. http://www.cica.ca/focus-on-practice-areas/governance-strategy-and-risk/directors-series/director-briefings/item66262.pdf*

[7] *20 Questions Directors Should Ask about Crisis Management, Doug Enns, FCA, C.Dir & Hugh Lindsay, FCA, CIP, Chartered Professional Accountants of Canada 2008. http://www.cica.ca/focus-on-practice-areas/governance-strategy-and-risk/directors-series/20-question-series/item60621.pdf*

Annex 1: ICGN Guidance

Anti-corruption Practices

Corporate Risk Oversight

Executive Remuneration

Gender Diversity on Boards

Integrated Business Reporting

Institutional Investor Responsibilities

Model Mandate: Contract Terms Between Asset Owners and Managers

Non-executive Director Remuneration

Political Lobbying and Donations

Securities Lending Code of Best Practice

What investors want from financial reporting

ICGN
International Corporate Governance Network

Contact

Email: **secretariat@icgn.org**

Phone: **+44 (0) 207 612 7011**

Web: **www.icgn.org**

Post: ICGN Secretariat, Saffron House, 6 -10 Kirby Street, London, EC1N 8TS, UK