Control Environment Toolkit

 Risk Governance

Specimen Risk Management Committee Charter

© International Finance Corporation 2023. All rights reserved.

2121 Pennsylvania Avenue, N.W.

Washington, D.C. 20433

Internet: www.ifc.org

The material in this work is copyrighted. Copying and/or transmitting portions or all of this work without permission may be a violation of applicable law. IFC encourages dissemination of its work and will normally grant permission to reproduce portions of the work promptly, and when the reproduction is for educational and non-commercial purposes, without a fee, subject to such attributions and notices as we may reasonably require.

IFC does not guarantee the accuracy, reliability, or completeness of the content included in this work, or for the conclusions or judgments described herein, and accepts no responsibility or liability for any omissions or errors (including, without limitation, typographical errors and technical errors) in the content whatsoever or for reliance thereon. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of the World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The findings, interpretations, and conclusions expressed in this volume do not necessarily reflect the views of the Executive Directors of the World Bank or the governments they represent.

The contents of this work are intended for general informational purposes only and are not intended to constitute legal, securities, or investment advice, an opinion regarding the appropriateness of any investment, or a solicitation of any type. IFC or its affiliates may have an investment in, provide other advice or services to, or otherwise have a financial interest in, certain of the companies and parties (including named herein).

All other queries on rights and licenses, including subsidiary rights, should be addressed to IFC’s Corporate Relations Department, 2121 Pennsylvania Avenue, NW, Washington, DC 20433 USA.

International Finance Corporation is an international organization established by Articles of Agreement among its member countries, and a member of the World Bank Group. All names, logos, and trademarks are the property of IFC, and you may not use any of such materials for any purpose without the express written consent of IFC. Additionally, “International Finance Corporation” and “IFC” are registered trademarks of IFC and are protected under international law.

**IFC Specimen Documents   
for Nonfinancial Institutions –   
Risk Management Committee Charter   
for Nonfinancial Institutions**

*Approved*

*by decision of the Board of Directors*

*of* [the Company] *“\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_”*

*Board Minutes*

*No \_\_\_\_\_\_\_\_\_\_\_\_*

*of \_\_\_\_\_\_\_\_\_ 20\_\_*

*Signature of the Chairperson of the Board*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*dated this \_\_ day of \_\_\_\_\_\_\_\_, 20\_\_*

[The Company Seal]

*Risk Management Committee Charter*

*of* [the Company]

*“\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_”*

Table of Contents

1. General Provision 5

2. Definitions 5

3. Purposes of the Committee 7

4. Authority and Resources 8

5. The Risk Governance Structure 8

6. Responsibilities 9

7. Membership and Organization 11

8. Meeting Attendance and Notice 12

9. Relationship with Other Board Committees 13

10. Reporting to the Board and Shareholders 14

11. Communicating to External Stakeholders 14

**Color Coding:**

**Provisions in black:** “Basic” provisions are considered the minimum requirements with which the organization should comply.

Provisions in green: “Intermediate Practices” outline additional steps to strengthen corporate governance and risk management in the organization.

**Provisions in blue:**  “Good International Practices” indicate that the organization has more-mature corporate governance and a more-established risk management system.

Provisions in red: “Leadership” provisions indicate that the organization aspires to conform with the highest international corporate governance and risk management practices.

1. General Provision
   1. The Risk Management Committee (“Committee”) is a board-level committee established by resolution of the Board of Directors (“Board”) to assist the Board in managing risk. Establishment of the Committee is incorporated into the company’s [corporate charter, articles of association, corporate governance policy, bylaws].
   2. This Charter defines the purpose, scope, and authority of the Committee and the responsibilities of Committee members, meeting procedures, and remuneration of members.
   3. The Charter reflects the Company’s compliance with COSO or International Standards Organization (ISO) 31000, which constitutes generally accepted international best practices in risk governance and management.
2. Definitions
   1. For the purposes of this Charter, the following terms shall have the following meanings.

|  |  |
| --- | --- |
| * + 1. Business Continuity Plan | A documented collection of procedures and information developed, compiled, and maintained in readiness for use during an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level. |
| * + 1. Business Continuity Planning | The process of developing prior arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption. The result of the planning process is the Business Continuity Plan. |
| * + 1. Climate Risk | Risk assessments based on formal analysis of the consequences of, likelihood of, and responses to impacts of [climate change](https://en.wikipedia.org/wiki/Climate_change) and how societal and environmental constraints shape adaptation options. |
| * + 1. Crisis Management | The process by which an organization manages the wider impact of any situation until it is under control or a full Business Continuity Plan is invoked. It can be used in situations in which the main activities are external, such as addressing malicious rumors, hostage taking, product failure, or product recall. |
| * + 1. Enterprise Risk Management | A process that the Board, management, and other personnel effect, applied strategically and across the enterprise and designed to identify potential events that may affect the entity, manage risk so that it remains within the enterprise’s risk appetite, and provide reasonable assurance regarding achievement of objectives. |
| * + 1. Environmental and Social (E&S) Risk | Risk of harm to people or the environment through inadequate or failed internal processes, people, or systems or through external events. |
| * + 1. Event | An internal or external incident that affects achievement of objectives. |
| * + 1. Impact | The effect of an event, which can be positive or negative. |
| * + 1. Non-Executive Director | A member of a Company's Board who is not a Company employee, which means that they do not engage in day-to-day management of the organization. A nonexecutive director is frequently independent, for which additional prerequisites must be met (see below). |
| * + 1. Internal Control | A process, effected by an entity’s board, management, and other personnel to provide reasonable assurance regarding the achievement of objectives in (a) effectiveness and efficiency of operations; (b) reliability of financial reporting; and (c) compliance with applicable laws and regulations. |
| * + 1. Key Risk Indicators | Metrics that organizations use to provide an early signal of increasing risk exposure in various areas of the enterprise. |
| * + 1. Legal Risk | Risk of a loss owing to unexpected application of a law or regulation, because a contract cannot be enforced, or from an unexpected lawsuit. |
| * + 1. Independent (Non-Executive) Directors | An Independent Director is a director who:   1. the Company or its Related Parties has not employed in the past 5 years; 2. is not, and is not affiliated with, a company that is an advisor or consultant to the Company or its Related Parties; 3. is not affiliated with a significant customer or supplier of the Company or its Related Parties; 4. has no personal service contracts with the Company, its Related Parties, or its senior management; 5. is not affiliated with a nonprofit organization that receives significant funding from the Company or its Related Parties; 6. is not employed as an executive of another company on whose board of directors any of the Company's executives serve; 7. is not a member of the immediate family of an individual who the Company or its Related Parties employs or has employed during the past 5 years as an executive officer; 8. is not, and has not in the past 5 years been, affiliated with or employed by a present or former auditor of the Company or of a Related Party; or 9. is not a controlling person of the Company (or member of a group of individuals or entities that collectively exercise effective control over the Company) or such person’s sibling, parent, grandparent, child, cousin, aunt, uncle, nephew, or niece; a spouse, widow, in-law, heir, legatee, or successor of any of the foregoing (or any trust or similar arrangement of which any such persons or a combination thereof are the sole beneficiaries); or the executor, administrator, or personal representative of any person described in this subparagraph who is deceased or legally incompetent, and for the purposes of this definition, a person shall be deemed to be "affiliated" with a party if such person (i) has a direct or indirect ownership interest in; or (ii) is employed by such party;. “Related Party” shall mean, with respect to the Company, any person or entity that controls, is controlled by, or is under common control with the Company. |
| * + 1. Operational Risk | Risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. |
| * + 1. Opportunity | Possibility that an event will occur and positively affect the achievement of objectives. |
| * + 1. Risk | Anything that can affect the ability of an enterprise to meet its objectives. |
| * + 1. Risk Analysis | A process intended to reveal the nature of potential risk and determine the level of risk. |
| * + 1. Risk Appetite | Broadly based level of risk the entity is willing to seek or accept in pursuit of long-term objectives. |
| * + 1. Risk Assessment | Process of identifying risks, assessing critical functions necessary to continue business operations, defining the controls in place to reduce exposure, and evaluating the cost of such controls. Risk assessment often involves an evaluation of the probability of a particular event. |
| * + 1. Risk Governance | Principles of good governance applied to identification, assessment, management, and communication of risk. It incorporates principles of accountability, participation, and transparency in establishing policies and structures to make and implement risk-related decisions. |
| * + 1. Risk Management | Coordinated activities to direct and control risk. |
| * + 1. Risk Management Framework | Complete set of components that provide the foundation and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization. |
| * + 1. Risk Management Policy | Statement of overall intent and direction related to risk management. |
| * + 1. Risk Management Process | Systematic application of policies, procedures, and practices to identify, analyze, evaluate, address, monitor, and review risk and to establish the context for these activities and to risk-related communications and consulting. |
| * + 1. Risk Measurement | Evaluation of likelihood and magnitude of a risk. |
| * + 1. Risk Tolerance | Boundaries of risk taking outside of which the organization is not prepared to venture in pursuit of long-term objectives. |
| * + 1. Sensitive Industries | Industries that are materially exposed to high-intensity greenhouse gas emissions or to the effects of direct or indirect impacts of climate change. Examples of sensitive industries include aviation, oil, gas, mining, heavy industry (steel, cement), chemical manufacturing, and large agro-commodity production or processing. These are primarily industries with high emission intensity in which climate action focuses on mitigation measures. There are additional weather-dependent industries in which changes in climate can affect operation or production for which climate change adaptation measures are critical to reducing the material impact on financial or E&S performance. |
| * + 1. Strategic Risk | Risk of loss resulting from failure in execution of a business strategy or failure to respond to a changing business environment. |
| * + 1. Threat | An event with potentially adverse consequences. |

1. Purpose of the Committee
   1. The purpose of the Committee is to assist the Board in overseeing, monitoring, and reviewing the effectiveness of the Company’s risk management framework and other matters related to management of strategic risk, business risk, climate and E&S risk, and operational risk inherent in the Company’s business. Specifically, the Committee shall:
      1. Oversee implementation of a risk management framework;
      2. Oversee and monitor senior management’s performance in implementing the Company’s risk management policy and related procedures and practices based on the risk management framework;
      3. Review and recommend for Board approval a risk management policy and risk management strategies; and
      4. Adhere to international standards for best practices in corporate governance and risk management.
2. Authority and Resources
   1. The Board authorizes the Committee to discharge its duties within the terms of this Charter. The Committee shall have the right to:
      1. Seek any information it requires from any employee or member of management in conducting its work;
      2. Request that management appear before it to account for management’s delegated responsibilities in respect of risk management;
      3. Obtain outside independent professional advice and services (e.g., risk management consultants, financial experts, legal counsel) and secure attendance of outside experts with relevant experience and expertise as it deems necessary in performance of its duties; and
      4. Perform any other duties that the Board requires within the scope of the authority of the Committee as set forth herein.
   2. The proposals that the Committee develops are recommendations only and thus nonbinding on the Board unless adopted.
   3. The Committee shall receive an annual budget to discharge its duties and, subject to approval of the Board, has the right to access additional funds if required.
3. Risk Governance Structure
   1. The risk management process forms part of the corporate governance framework of the Company. The Board and Company management have established a risk governance structure to manage major risks that the Company faces, oversee operation of the risk governance framework, and provide reasonable assurance that the Company’s key objectives will be achieved. Key risks that the Company measures and manages are strategic risk, business risk, climate and E&S risk, and operational risk, as well as other risks that emerge from time to time.
   2. The Board shall adopt the “Three Lines Model”[[1]](#footnote-1) of Risk Governance, with management the first line of defense, the Risk Management Committee and the chief risk officer the second line of defense, and internal audit the third line of defense (Annex 1).
   3. As the first line of defense, management is responsible for day-to-day management of risks that are integrated with operations and decision-making processes.
   4. As the second line of defense, the Board delegates the Committee to oversee risk management. The Committee sets risk management policies, receives reports on their performance, and reviews risks that require the Board’s attention.
   5. The Risk Management Department, which is responsible for risk measurement and risk assessment at the transaction level, reports to the Committee.
   6. A Chief Risk Officer (CRO) or an executive with an equivalent title heads the Risk Management Department, is accountable to the Committee, is responsible and accountable for execution of the risk management policy and development of risk management strategies, and has the following responsibilities:
      1. Ensure the accuracy, completeness, and currency of the risk register;
      2. Ensure that adequate, feasible risk control measures are in place; and
      3. Advise the Board, the Committee, and management on technical matters related to risk management.
   7. The Audit Committee, internal auditor, and External Auditor provide independent assurance on the risk management process—the third line of defense. Refer to the Audit Committee Charter for its responsibilities.
4. Responsibilities
   1. The Committee assists the Board in overseeing the risk management framework and systems of the Company and ensures that all key strategic risks are managed in accordance with the relevant policies and in line with the risk appetite levels and risk tolerance limits that the Board determines (based on recommendations from the Committee).
   2. ***Risk Governance***
      1. The Committee oversees the setting of policies and strategies to manage risk. Specifically, the Committee shall:
         1. Oversee development, implementation, and management of the risk management framework to meet the Company’s objectives, legal requirements, and other external requirements (e.g., those of rating agencies);
         2. Review and recommend for Board approval significant risk management policies and direct management to develop and implement additional policies relating to risk management at the operations level;
         3. Oversee development of an overall risk management strategy to guide the company in meeting its business objectives while managing risk effectively;
         4. Oversee implementation of the risk management program and review its quality and soundness;
         5. [For sensitive industries] oversee periodic review of the effectiveness of the Company’s E&S risk management system;
         6. Ensure that climate risks are integrated into the organization’s overall risk framework;
         7. Oversee development of a business continuity strategy and plan, to be implemented in the event of business interruption;
         8. [For all industries] oversee periodic review of effectiveness of the company’s E&S risk management system;
         9. Ensure that adequate climate mitigation and adaptation measures are implemented;
         10. Conduct or be involved in annual scenario analysis to evaluate the Company's resilience to climate change;
         11. Ensure that the Committee adopts best practices in corporate governance in discharging its duties in governance of risk management;
         12. Oversee adoption and implementation of an enterprise-wide risk management framework, policies, and processes, according to international standards such as The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management Framework (COSO) or the International Organization for Standardization (ISO) 31000, to facilitate management of the Company’s risks in a coordinated, systematic manner and to integrate risk management into the business-planning and decision-making processes;
         13. Review periodically, with input from the internal auditor, CRO, or external advisors, the effectiveness of the risk management systems; and
         14. Keep abreast of developments in international standards and best practices in risk governance and risk management and make recommendations to the Board when changes are appropriate for the Company.
   3. ***Enterprise-Wide Risk Appetite Levels and Risk Tolerance Limits***
      1. The Committee advises the Board on the Company’s risk appetite level and risk tolerance limit.
      2. The Committee shall review at least annually the Company’s risk appetite level and risk tolerance limit based on changes and developments in the business, laws, and external economic and business environment and make recommendations to the Board as appropriate.
      3. The Committee shall initiate a review of the risk appetite level and risk tolerance limit immediately if a major event occurs that is considered to have major impacts on the Company.
   4. ***Enterprise-Wide Risk Identification, Assessment, Control and Monitoring***
      1. The Committee shall ensure that management has implemented a comprehensive risk management process in accordance with the Company’s policy and oversee adoption of international standards for risk management in general (e.g., COSO, ISO 31000). The Committee shall:
         1. Oversee establishment of a risk register with clearly defined risk categories and risks;
         2. Oversee development of key risk indicators to monitor key risks identified;
         3. Review risk identification and assessment methodologies to obtain reasonable assurance of the completeness and accuracy of the risk register;
         4. Review management’s assessment of the portfolio of risks against the Company’s risk appetite and strategic plan;
         5. Be apprised of significant risks in terms of their measurement, control measures applied, and trends and ensure that management is responding to these risks appropriately and competently with specific risk responses;
         6. Monitor key risk indicators that management reports and determine requisite actions for significant variances;
         7. Regularly receive disaggregated data on major risk categories from responsible managers;
         8. Review and monitor actions taken with respect to compliance and internal audit reports when they are relevant to the risk function;
         9. Oversee the process of identifying the top 10 strategic and operational risks that the Company faces;
         10. Monitor risks across relevant groups, structures, or affiliates as warranted along the supply chain; and
         11. Review developments and changes in legal requirements and the business environment and recommend strategies to the Board to address them.
   5. ***Risk Communication and Reporting***
      1. The Committee shall recommend policies to the Board and establish the process and criteria for communicating and reporting risk information internally and externally:
         1. Ensure that risks are clearly categorized and defined and that one set of definitions is used throughout the Company;
         2. Determine escalation criteria for risk reporting and ensure that all significant risks are communicated to appropriate management levels and that the most significant risks are escalated to the Board;
         3. Review the format and content of risk management information reported to the Board and the Committee;
         4. Ensure that management has provided complete, accurate risk information and has made all reasonable efforts to identify and assess key risks;
         5. Review and recommend policies and procedures for communicating risk information to external stakeholders, including but not limited to shareholders, the public, and the media, under normal circumstances and in crisis situations (refer to Section 11); and
         6. Ensure that E&S risk management activities and climate risks are included in reports to the Board.
      2. The CRO shall keep the Committee informed of any concerns related to the top 10 strategic and operational risks and their impacts on the Company’s ability to meet its business objectives.
   6. ***Appointment and Dismissal of the CRO***
      1. The Committee shall ensure that the CRO has adequate authority, resources, and support to fulfill their responsibilities.
      2. The Committee shall endorse the job description of the CRO. Committee members shall interview the final shortlisted candidates during selection of the CRO. Appointment and dismissal of CRO shall require approval from the Committee.
   7. ***Performance Evaluation***
      1. The format and frequency of the Committee’s performance evaluations shall be the same as those of the Board, in accordance with prevailing Board policy.
      2. The Committee shall review the Charter annually and recommend any amendments to the Board.
      3. The Committee shall conduct annual internal evaluations of its work and performance during the previous year.
      4. As the Company’s corporate governance matures, external consultants shall conduct an independent evaluation of the effectiveness of the Committee as a whole by every 3 years.
5. Membership and Organization
   1. ***Composition***
      1. The Committee shall consist of a minimum of three members that shall be selected from among the nonexecutive directors on the Board [at least one-third of whom shall be independent].
      2. If there are insufficient qualified nonexecutive directors on the Board, at a minimum, the Chairperson shall be an independent nonexecutive director.
      3. At least one Committee member shall understand E&S risks.
      4. At least one director shall have experience analyzing and interpreting climate risks and opportunities.
      5. If the Company does business in sensitive industries, at least one Committee member shall have in-depth knowledge of the E&S risks related to those industries.
      6. If the Company does business in climate-sensitive industries, one director or more shall have relevant in-depth knowledge of climate risks and opportunities.
      7. One member of the audit committee shall be a member of the Committee, but no more than one Board member should sit on both the Audit Committee and the Risk Management Committee.
      8. The Committee may invite senior management of the Company or others to attend a Committee meeting if the Committee considers it appropriate.
   2. ***Committee Chairperson***
      1. The Chair of the Board shall appoint the Committee Chair, or the Committee shall elect its Chair from among the Committee members.
      2. The Committee Chair will convene and chair Committee meetings. In the absence of the Chair, based on majority vote of members present, another Committee member shall chair the meeting.
      3. The Committee Chair should be an independent nonexecutive director that the Board appoint on the recommendation of the Nomination Committee.
      4. The Committee Chair shall have the necessary skills and knowledge to oversee the Company’s risk management systems and practices and shall preferably have experience in one or more of the industries in which the Company operates and in governing and managing risk in those industries.
      5. The Chair shall have the stature and experience to lead the Committee and communicate effectively with the Chair of the Board, other Board members, and senior management.
   3. ***Nomination, Appointment, and Dismissal***
      1. Committee members shall be current Board members, and the Board shall appoint them through nomination by the [Board or the Corporate Governance or Nomination Committee]. Members shall be appointed for a term of 1 year, subject to renewal. Members with less than 75% attendance at Committee meetings shall not be considered for reappointment.
      2. The [Corporate Governance or Nomination Committee] shall recommend to the Board early termination of a Committee member in accordance with policies and procedures set out in the Company’s corporate governance policy.
   4. ***Individual Committee Member Qualifications***
      1. Committee members shall have the necessary skills, expertise, and knowledge in the area of risk management. At least one member, if not the Chair, shall have direct experience in governing and managing risk in the Company’s industry and with E&S and climate risks.
      2. Collectively, the Committee shall have sufficient knowledge of the Company’s major business areas and strategies, and material risks associated with those business areas, to assess the effectiveness of the Company’s risk management system and recommend improvements in the system to the Board.
   5. ***Training***
      1. The Committee Chair shall from time to time review the competency of Committee members in discharging their duties and ensure that training and education are provided to them as part of the induction program for new members and on an on-going basis as new risk categories or new standards emerge.
   6. ***Remuneration***
      1. Committee members shall be remunerated solely for fulfilling their obligations to the Committee. The Board policy on compensation of Board members shall govern remuneration.
      2. The Committee Chair and other Committee members shall receive an annual emolument, in addition to their fees as a member of the Board, to reflect their additional responsibilities. Additional amounts, such as per-meeting fees or disbursements such as travel expenses, shall be payable according to the relevant policy.
      3. In consultation with the Corporate Governance or Nomination Committee, the Remuneration Committee shall recommend remuneration and payment policies that the Board has endorsed and have been adequately disclosed in annual reports.
   7. ***Secretary***
      1. A member of the Company’s staff shall be appointed as Secretary to assist the Committee Chair in preparing agendas for Committee meetings and distributing them to members in advance, together with supporting documents. The Secretary shall also attend meetings to take minutes, ensure that meetings are conducted in accordance with the relevant corporate governance policies, and maintain and distribute Committee meeting minutes. The Company Secretary shall be the secretary of the Committee.
6. Meeting Attendance and Notice
   1. ***Frequency of Meetings***
      1. Meetings may be held as often as necessary to conduct the Committee’s functions and duties properly and in a timely manner. At a minimum, [the Committee shall meet semiannually within the fiscal year, with additional meetings as necessary, or the Committee shall meet four times per fiscal year, with meetings scheduled every 3 months and additional meetings as necessary]. Committee meetings shall be included in the annual calendar of regular Board and Committee meetings that the Board approves at the beginning of each fiscal year.
      2. [The Committee Chair may convene *ad hoc* meetings and The Committee Chair or any two Committee members may convene additional meetings if required]. The Chair of the Board, chair of the audit committee, chief executive officer, chief financial officer, or CRO may also request that a meeting be convened.
   2. ***Notice of Meeting***
      1. Unless otherwise agreed, notice of each meeting confirming the venue, time, and date shall be given to members and any other persons required to attend no less than 48 hours before the meeting or no less than 1 week before the meeting].
      2. The meeting agenda shall be distributed to members together with the meeting notice. Should the Committee Chair decide that confidentiality is required with respect to an agenda item, a general description of the subject to be discussed and an explanation of the need for confidentiality shall be included in the agenda.
   3. ***Conduct of Meetings***
      1. Meetings shall be the principal form of conducting the work and activities of the Committee.
      2. Quorum shall be a simple majority (e.g., presence of two of three members). A duly convened Committee meeting at which a quorum is present shall be competent to exercise any of the authorities, powers, and discretions vested in or exercisable by the Committee.
      3. Meetings shall be conducted in accordance with the provisions of the Company’s Corporate Charter, Articles of Association, or Corporate Governance Policy governing the proceedings of meetings.
      4. Meetings may be held in person, by telephone, online, or other means of electronic communication agreeable to the Committee, provided that each member in attendance has the opportunity and means to express their views on each agenda item. The Committee shall have the discretion to act by unanimous written consent in lieu of a meeting.
      5. Independent members of the Committee (independent nonexecutive directors and nonexecutive directors) shall meet at least once per year with no executive officers present.
   4. ***Minutes of Meetings***
      1. The Secretary shall record the proceedings and resolutions of all Committee meetings, including the names of those present and absent.
      2. Committee meeting minutes shall be prepared and circulated to all Committee members.
      3. Before each Committee meeting, the most recent meeting minutes shall be distributed to members in advance and subject to approval at the meeting. Members of the full Board shall have access to the approved minutes of the Committee.
7. Relationship with Other Board Committees
   1. The Committee Chair shall work with the Audit Committee Chair to ensure that the work of the two committees is complementary and without unnecessary overlap in activities with respect to risk management. The Committee shall rely on the Audit Committee to provide assurance that internal controls in relation to each of the key risks are in place.
   2. The Committee Chair shall coordinate with the Remuneration Committee Chair to ensure that the Company’s compensation and benefits arrangements provide incentives to senior executives to enhance the value of the Company but do not encourage them to take excessive risks to the detriment of the interests of shareholders.
8. Reporting to the Board and Shareholders
   1. The Committee Chair shall report to the Board at each Board meeting on the activities and major decisions of the Committee since the previous Board meeting. Approved minutes of the Committee meetings shall also be made available to the Board.
   2. [For all industries,] E&S risk-management activities and climate risk management activities shall be included into reports to the Board.
   3. The Committee, as part of the Board, shall be accountable to the shareholders. The Company’s performance in risk management shall be reported in the Annual Report.
   4. The Committee shall submit an Annual Report to the Board on the activities of the Committee during the year that describes the status of the Company’s risk management, areas requiring improvement, and the Committee’s recommendations for addressing areas requiring improvement.
   5. The Committee Chair (or another Committee member if the Chair is unable to attend or a duly appointed delegate if no Committee members are able to attend) shall attend the Company’s Annual General Meeting to respond to any questions from shareholders regarding the Committee’s activities.
   6. The Annual Report shall include a discussion of the Company’s risk management activities, including E&S risk-management activities.
   7. As part of its Annual Report, the Company shall prepare integrated financial, E&S, and climate risk reports.
9. Communicating to External Stakeholders
   1. Transparency is an essential component of sound corporate governance and of risk management. The Committee shall ensure, as part of its corporate communications policy, that policies, procedures, and responsibilities with respect to communicating risk information to key external stakeholders under normal circumstances and in crisis situations are in place. Such communications shall be part of the corporate communications policy and plan.
   2. Under normal circumstances, the Committee shall ensure routine timely disclosure of risk management policies and practices and foreseeable risk factors, in accordance with relevant legal and business requirements.

If the Company is publicly listed, communication and disclosure of risk information to external parties, particularly information considered price sensitive, shall adhere to the disclosure requirements in the relevant listing rules.

* 1. The Committee shall ensure that the crisis management plan and business continuity plan are ready for execution and provide details regarding organization, procedures, checklists, and templates to enable efficient, effective response to a crisis; continuity of critical business functions; and full recovery of business operations. The Committee shall endorse the plans and determine the criteria for invoking them, consistent with the Company’s risk appetite and risk tolerance limits.
  2. The corporate communications department shall be responsible for all corporate communications. The Committee shall advise the Board on assignment of spokespersons to ensure consistency, accuracy, and appropriateness of communications. The Board Chair, chief executive officer, chief financial officer, or head of corporate communications shall be the spokesperson with respect to predefined issues.

### Annex 1: The IIA’s Three Lines Model[[2]](#footnote-2)

Diagram, text, timeline

Description automatically generated

2121 Pennsylvania Avenue, NW

Washington, DC 20433 USA

Tel: +1 (202) 458-8097



www.ifc.org/corporategovernance

www.ifc.org/sustainability February 2023

1. The Institute of Internal Audit (IIA) Three Lines Model. [↑](#footnote-ref-1)
2. Available at: https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf. [↑](#footnote-ref-2)