Control Environment Toolkit

Charter Assessment Tool:

Risk Management Committee



© 2023 International Finance Corporation. All rights reserved.

2121 Pennsylvania Avenue, NW

Washington, DC 20433 USA

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.

 Control Environment Toolkit

Risk Governance

IV. Assessment tools for non-financial institutions – risk management committee charter assessment tool: part of IFC’s advanced methodology for enterprises other than financial institutions

|  | 1. Basic
 | **+** | 1. Intermediate Practices
 | **+** | 1. Good International Practices
 | **+** | 1. Leadership
 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I. Establishment[[1]](#footnote-2) | 1. Any written document, including a Board resolution
 | 1. Incorporate into By-Laws[[2]](#footnote-3) or corporate governance guidelines
 | 1. Incorporate into Corporate Charter or Articles of Association
 | 1. Same[[3]](#footnote-4)
 |
| II. Purpose | 1. Establish Company’s risk policies, including risk tolerances, consistent with risk management program (see also XIV)
 | 1. Same, *and ensure that senior management takes necessary steps to identify, measure, monitor, and control risk*
 | 1. Same
2. Ensure that major concerns are escalated to risk management committee or Board for discussion
 | 1. Same
2. Same
3. Establish enterprise-wide risk management framework for all companies in the group and at all levels, based on international best practices such as Committee of Sponsoring Organizations of the Treadway Commission and International Standards Organization 31000
 |
| III. Composition | 1. At least three board members
2. Material presence of non-executive board members
 | 1. Same
2. Same, *but Company Secretary performs role*
3. All committee members are non-executive Board members[[4]](#footnote-5)
4. At least one Board member has understanding of environmental and social (E&S) risk
5. At least one director has experience analyzing and interpreting climate risks and opportunities
 | 1. Same
2. Same
3. Same, *and at least one-third are independent non-executive directors*
4. Same, *and for climate-sensitive industries,[[5]](#footnote-6) this Board member has in-depth knowledge of climate and E&S risks and opportunities related to the industry*
5. Same, *and for sensitive industries, one or more directors has relevant in-depth knowledge of climate risks and opportunities*
 | 1. Same
2. Same
3. All members are independent non-executive directors
4. Same
5. Same
6. Rotation of members
7. Less than 75% attendance at committee meetings in 1 year is automatic threshold for non-reappointment
8. Limit on number of memberships on other Board committees
9. No more than one committee member serves on both the risk management and audit committees
 |
| IV. Committee Chair | 1. Appointed by Board or non-executive Chair of the Board or elected from among members of Committee
 | 1. Same
2. Non-executive director
3. Has skills necessary to oversee Company’s risk management system and practices
 | 1. Same
2. Same
3. Same, *and has experience governing risk in a relevant industry*
4. Has stature and skills to communicate effectively with Chair of the Board, Chair of Audit Committee, and other directors
 | 1. Same
2. Same, *and is an independent board* *member*
3. Same
4. Same
5. Has business experience to see big picture and steer Committee through major or strategic risks
 |
| V. Commitment and Professional Development of Committee Members | 1. Committee members have business or professional experience
2. Committee members have time and desire to fulfill Committee obligations
 | 1. Same
2. Same
 | 1. Same, *and have skills and knowledge to oversee Company’s risk management systems and practices*
2. Same
3. Induction training provided to new Committee members
 | 1. Same
2. Same
3. Same
4. Periodic professional education and training provided for Committee members
5. Less than 75% attendance at Committee meetings in 1 year set as threshold for non-reappointment
6. Competency of members in discharging duties reviewed from time to time and appropriate training provided
 |
| VI. Appointment of Members | 1. Board members
2. Board, Chair of Board, or Corporate Governance or Nominations Committee
 | 1. Same
2. Same
3. Fixed terms, preferably annual but not exceeding Board terms
 | 1. Same
2. Same, *and* *recommended by Nominations Committee and approved by Board*
3. One-year renewable terms
 | 1. Same
2. Same
3. Same
4. Same
 |
| VII. Remuneration (in Addition to Compensation for Work as Board Member)[[6]](#footnote-7) | 1. Solely related to fulfilling obligations of a committee member (no form of payment that would compromise independence, e.g., salary, consulting, finder’s fee)
 | 1. Same, *but* *payment as Committee fees or meeting fees is preferred form*
2. Adequate level of payment to create expectation of responsibility
 | 1. Annual Committee fees
2. Same
3. Additional per-meeting fees
4. Additional fee for Chair
 | 1. Same
2. Same
3. Same
4. Same
5. Remuneration that remuneration committee recommends and board approves
 |
| VIII. Meetings | 1. Held at least semi-annually
2. Committee Chair may call *ad hoc* meetings
 | 1. At least quarterly
2. Same, *and by any two committee members*
3. Approved annual calendar of regular meetings[[7]](#footnote-8)
 | 1. Same
2. Same, *and Chair of Board, chief executive officer (CEO), chief financial officer, or chief risk officer (CRO) may request[[8]](#footnote-9)*
3. Same
4. Meetings may be in person, by telephone, online, or by other means of electronic communication agreeable to committee and in line with overall policies in conducting Board-level meetings
5. Ability to act by unanimous written consent
 | 1. Same
2. Same
3. Same
4. Same
5. Same
6. Independent members of Committee meet at least once a year without executive directors
 |
| IX. Attendance and Notice | 1. Quorum required
2. Advance notice required; may be waived with unanimous written consent
 | 1. Same, *and simple majority as a minimum*
2. Same
3. Approved annual calendar of regular meetings
4. Minutes prepared and distributed to committee members; Board has access to review minutes
5. Agenda and related materials provided in advance unless Chair (or other convener) believes confidentiality requires otherwise, in which case a general description of subject of meeting is circulated, with a statement from Chair as to reasons for confidentiality
 | 1. Same
2. Same, *and with minimum 48 hours’ notice*
3. Same
4. Same, *together with minutes of the last meeting*
5. CRO and other executive officers attend meetings if invited
6. Chief of Internal Audit, External Auditor, and chief compliance officer given notice of all meetings
 | 1. Same
2. Same, *and with minimum 1 week’s notice*
3. Same
4. Same
5. Same
6. Same
 |
| X. Reporting to Board and Shareholders | 1. Oral or written reports submitted to Board as needed
2. For sensitive industries, E&S risk management activities included in reports to Board
 | 1. Written reports or minutes submitted to Board after each Committee meeting
2. For all industries, E&S risk management activities included in reports to Board
3. Climate risks included in reports to Board
4. Annual written report submitted to Board
 | 1. Same
2. Same
3. Same, *and includes adequate climate mitigation and adaptation measures*
4. Report on Company’s risk management activities included in Annual Report
 | 1. Same
2. Same
3. Same, *and includes annual scenario analysis to evaluate Company’s resilience*
4. Same, *with qualitative and quantitative data enabling shareholders and public to understand Company’s risk profile and policies*
5. Committee Chair or representative attends Annual General Meeting to answer shareholder questions on work and activities of Committee
6. Integrated financial, environmental, and social report prepared annually
7. Task Force on Climate-related Financial Disclosures report or report pursuant to comparable framework or integrated report prepared annually and provides information on climate risk and opportunities
 |
| XI. Communication to External Stakeholders | 1. Regular communication of risk information to key external stakeholders (e.g., public, affected communities, media, government)
 | 1. Same, *with policies and plans in place for corporate communications*
 | 1. Same
2. Committee endorses crisis management plan and business continuity plan
3. External communication is coordinated by the corporate communications department, with responsibilities, including those of spokespersons in various situations, clearly defined
 | 1. Same
2. Same, *and* *plan is periodically tested and ready to execute*
3. Same
4. Integrated financial, environmental, and social performance report and climate risk report provided to public as part of annual reporting
 |
| XII. Evaluation[[9]](#footnote-10) |  | 1. Committee’s work during past year discussed annually at a Board meeting
2. Charter reviewed annually
 | 1. Same
2. Same
3. Work and performance of Committee evaluated annually
4. Effectiveness of Committee, including processes and procedures, evaluated annually
 | 1. Same
2. Same
3. Same
4. Same
5. External consultants independently evaluate Committee’s effectiveness every 3 years
 |
| XIII. Authority and Resources | 1. Committee has access to all internal resources
 | 1. Same, *and may request that any staff member attend Committee’s meetings to answer questions related to risk management*
2. Committee makes recommendations regarding hiring of outside resources (e.g., risk management consultants, counsel, E&S or climate risk experts) as needed
 | 1. Same, *without necessarily going through hierarchy (although hierarchy should be respected absent compelling reasons not to do so)*
2. *Committee has right to hire outside resources without executive approval*
3. Committee may authorize or conduct any investigation within its area of responsibility, has the right to hire independent experts for such investigations, and approves the terms of engagement; company pays for such investigations
4. Appointment and dismissal of CRO and approval of terms of reference of risk management function
 | 1. Same
2. Same
3. Same
4. Same
5. Committee has annual budget sufficient for its needs and the right to access additional funds in unforeseen circumstances
 |
| XIV. Responsibilities—Policies and Procedures | 1. Review and recommend to Board, in conjunction with executive officers, proposed risk tolerance levels for various risk categories or business areas
2. Oversee implementation of Company’s risk management infrastructure and control systems
3. Direct management (e.g., CEO and CRO) in developing and operating comprehensive risk management program based on policies and strategy that Board sets
 | 1. Same
2. Same
3. Same, *and oversee implementation of risk management program and review its quality and soundness*
4. Ensure that risk management department operates independently of any line business function
5. Ensure that management consults Committee on Company’s insurance and risk financing program as risk transfer measures
6. For sensitive industries, oversee periodic review of effectiveness of Company’s E&S risk management system
7. Ensure that climate risks integrated into Company’s overall risk framework
 | 1. Same, *and advise Board on approving maximum credit exposure for major clients to ensure diversification and review Company’s risk appetite annually and as circumstances require*
2. Same
3. Same
4. Same, *and ensue that risk measurement and management functions have adequate expertise and resources to fulfill responsibilities*
5. Same, *and review adequacy and coverage of insurance and risk financing program and present to Board for approval*
6. Oversee periodic review of effectiveness of Company’s E&S risk management system (for all industries)
7. Same, *and implement adequate climate mitigation and adaptation measures*
8. Review assumptions and methodology of risk assessment process and compilation of risk register to ensure that all risk concerns have been properly considered and evaluated
9. Review level of delegated authority
10. Oversee Company’s business continuity and recovery plans to ensure preparedness to continue critical operations and recover in event of business interruption
 | 1. Same
2. Same, *and oversee adoption and implementation of enterprise-wide risk management framework according to international best practices such as Committee of Sponsoring Organizations of the Treadway Commission or International Standards Organization 31000*
3. Same
4. Same
5. Same
6. Same
7. Same, *and conduct or be involved in annual scenario analysis to evaluate Company's resilience to climate change*
8. Same
9. Same
10. Same, *and ensure that business continuity plan is in line with international best practices*
11. Oversee periodic review of effectiveness of Company’s risk management systems in light of changes in legal requirements and business environment
12. Keep abreast of developments in international standards and best practices in risk governance and management
 |
| XV. Responsibilities—Specific Risk Reviews | 1. Regularly receive summary risk data from responsible managers (CEO, CRO) and compare data with risk policies adopted
 | 1. Same
2. Regularly receive disaggregated data on major risk categories from responsible managers (CEO, CRO)
3. Receive and act on compliance and internal audit reports relevant to risk management
 | 1. Same, *and receive reports on top 10 strategic and operational risks identified*
2. Same
3. Same
4. Oversee development of key risk indicators and receive regular reports on them from CRO
5. Review exposure to major clients, markets, countries, and economic sectors and recommend action
 | 1. Same
2. Same
3. Same
4. Same
5. Same
6. Same
7. Advise compensation committee on compensation for senior management from a risk perspective to ensure that executives are encouraged to achieve corporate objectives without taking unnecessary risk
 |

|  |  |
| --- | --- |
| Acceptable | Minimum acceptable practices in corporate governance and risk management. Elementary. Meets the basic and regulatory/legal requirements. Reflexive.  |
| Better | Taking further steps to strengthen corporate governance and risk management. More established. Beginning to form a system. Meeting some internal and external regulatory/legal requirements. |
| Desirable | Major contributor to improving corporate governance and risk management nationally. Established. A system is in place. Meets all internal and external requirements. Proactive and forward looking. Working toward best practices. |
| Best Practice | Conforms to international best practices in the industry. Well-established system. Risk management is integrated into corporate governance framework. Forward looking and focused on continuous improvement. |

2121 Pennsylvania Avenue, NW

Washington, DC 20433 USA

Tel: +1 (202) 458-8097



www.ifc.org/corporategovernance

www.ifc.org/sustainability February 2023

1. It may be acceptable, in the case of relatively small enterprises, that the Board have no formal “risk” committee but that the full Board regularly discusses risk philosophy and tolerance and reviews the adequacy of risk management as a routine part of its strategic and operational review. Alternately, the functions of the risk management committee can be combined with those of the audit committee, although given the different remit of the audit committee regarding financial reporting, internal controls, and compliance, this is a function that the full Board should assume, or in what is increasingly considered best practice, the Board should establish a separate risk management committee. [↑](#footnote-ref-2)
2. By-Laws refer to internal corporate documents that are not required to be filed externally (with a corporation’s registry or the regulator). [↑](#footnote-ref-3)
3. “Same” in a column means that the recommendation with the same number in the column immediately to the left is carried over into that column. If the recommendation is the same but with additions, the additions are in italics. [↑](#footnote-ref-4)
4. In jurisdictions with a “two-tier” board system, “nonexecutive directors” means members of the supervisory board. [↑](#footnote-ref-5)
5. Climate-sensitive industries are those that are materially exposed to high-intensity greenhouse gas emissions or 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 emissions intensity, in which climate action focuses on mitigation measures. There are additional weather-dependent industries in which changes in climate can affect operations or production, for which climate change adaptation measures are key to reduce the material impact on financial or E&S performance. [↑](#footnote-ref-6)
6. Executive director members of the risk management committee, if any, do not receive additional remuneration for their services to the committee. [↑](#footnote-ref-7)
7. In addition to regular committee meetings, additional meetings may be held whenever needed and appropriate, with the agenda set in advance. [↑](#footnote-ref-8)
8. The chief risk officer is the most senior executive responsible for implementing risk management systems and processes in the enterprise, based on frameworks and policies that the Board approves. Titles such as head of risk management refer to the same role. Although the chief executive officer or chief financial officer may assume the role in some organizations, it is increasingly considered best practice to create a separate position directly accountable to the Board via the risk management committee. [↑](#footnote-ref-9)
9. The Corporate Governance/Nominations Committee may coordinate evaluation of Board and all committees at some companies. [↑](#footnote-ref-10)