Annex V: Non-financial risk policy

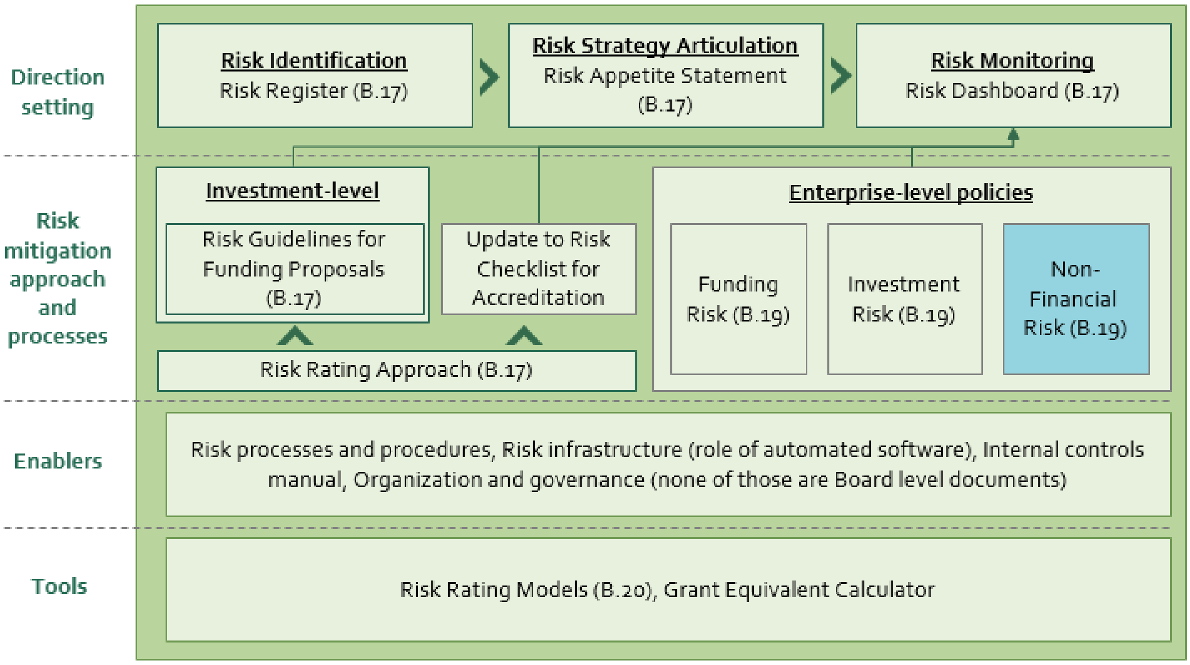
I. Introduction

1. This document presents a critical element of the Risk Management Framework ("RMF"), the policy governing non-financial risk management for the Green Climate Fund ("GCF").

II. Objectives and scope

2. This document, the Non-financial Risk Policy ("policy"), is a part of the comprehensive RMF – the components of the framework are presented below in Figure 2.

Figure 2: RMF components


Direction setting
Risk Identification
Risk Register (B.17)
Risk Strategy Articulation
Risk Appetite Statement (B.17)
Risk Monitoring
Risk Dashboard (B.17)
Risk mitigation approach and processes
Investment-level
Risk Guidelines for Funding Proposals (B.17)
Update to Risk Checklist for Accreditation
Risk Rating Approach (B.17)
Enterprise-level policies
Funding Risk (B.19)
Investment Risk (B.19)
Non-Financial Risk (B.19)
Enablers
Risk processes and procedures, Risk infrastructure (role of automated software), Internal controls manual, Organization and governance (none of those are Board level documents)
Tools
Risk Rating Models (B.20), Grant Equivalent Calculator

3. Non-financial Risk is defined as the potential for financial and non-financial losses arising from the failure of people, process, or technology or the impact of external events. It covers the following risk types defined in the Risk Register:

(a) **GCF Operational Process Error Risk:** Failure to meet the GCF's internal operations standards or non-compliance with external requirements (such as country laws or international agreements) that affect operations activities;

(b) **Staffing Risk:** Operational failures, losses and other disruptions arising from the staffing model of the GCF, including staff headcount level and external consultants, as well as from problems with recruitment, retention, succession planning, development, integrity and morale among the GCF staff;

(c) **Disasters and Other Events Risk:** Disruption of business due to natural or man-made catastrophic disasters;

(d) **IT Systems Failure Risk:** Disruption of business due to unavailability / inaccessibility of IT infrastructure and applications;

(e) **Cyber Attack Risk:** Misappropriation of internal data and/or information by a third party through IT means,[1] such as system security breach, hacking, phishing attacks, cybercrime, and malware / virus attacks; and

(f) **Reputation Risk:** Adverse perception which has a material effect on the credibility of the GCF (beyond the reputational damage which may be incurred due to one of the other risks in the Risk Register).

4. IT Systems Failure Risk and Cyber Attack Risk are hereinafter collectively referred to as "IT Risk".

5. The management approach to Disasters and Other Events Risk is described under Business Continuity Management ("BCM") in Section IV of this policy. BCM is a broader programme aimed at ensuring business continuity through the prevention and mitigation of Operational and IT Risk events.

6. This policy design is guided by the following principles:

(a) Ensuring sustainable viability for the GCF and enabling the GCF to meet its mission of promoting paradigm shift towards low-emission and climate-resilient development pathways;

(b) Adhering to the GCF's Risk Appetite Statement (part of the RMF) for Operational and IT Risk and Reputation Risk;

(c) Establishing fit for purpose controls and ensuring efficiency in risk management; and

(d) Allocating roles and responsibilities:

(i) **First Level of Responsibility ("First Level"):** The first responsibility of risk management and control is with the accountable units who are the primary owners and managers of risk; there may be multiple units within the Secretariat that form the First Level of Responsibility;

(ii) **Second Level of Responsibility ("Second Level"):** For each risk, there is a Second Level of Responsibility, or a control function independent of the First Level, to ensure risks are managed given asymmetric incentives, short-termism, and optimism of risk takers; there may be multiple units within the Secretariat that form the Second Level of Responsibility; and

(iii) **Third Level of Responsibility ("Third Level"):** The Third Level of Responsibility focuses on review of the actions and interactions of the risk taker and risk controller, and assurance that the RMF is operating as intended.

7. The detailed roles and responsibilities of the First and Second Levels are set out in sections III, IV, V, and VI below. The Third Level will develop and perform scheduled and ad-hoc audits, reviews, and assurance engagements, in order to gain assurance that the design and implementation of policies and procedures by the First and Second Levels are managing the GCF's risks appropriately.

III. Roles and Responsibilities: GCF Operational Process Error Risks and IT Risks

[1] Cyber attack risk could include falsification of internal data and/or information through IT means. This risk could also be created by the actions of internal parties.

8. Operational Process Error Risk arises from all GCF's activities. The following are the GCF's key activities and functions responsible (which the Secretariat deems most appropriate).[2] The Secretariat is responsible for nominating the Operational Risk Owners for all operational processes. The Operational Risk Owners are defined as the representatives of the First Level of Responsibility for operational process error risk:

(a) Accreditation process: Division of Country Programming ("DCP");

(b) Funding Proposal ("FP", "proposal") review process: Private Sector Facility ("PSF") and Division of Mitigation and Adaptation ("DMA"), for private and public proposals, respectively;

(c) Interim processes between Funding Proposal approval and signing a Funded Activity Agreement ("FAA"): PSF, DMA or DCP with the Office of the General Counsel ("OGC");

(d) Disbursement process: Chief Financial Officer ("CFO"); and

(e) Monitoring and evaluation: Portfolio Monitoring Unit ("PMU").

9. Other processes requiring an Operational Risk Owner include: Review process for other proposal types (PPFs, Readiness),[3] Human Resources ("HR") processes, Procurement processes, and other Finance processes (such as cash flow management and FX hedging).

10. Operational Risk Owners for operational process error risks are responsible for the following:

(a) Providing information to the Second Level required to populate the Operational Risk section of the Risk Dashboard, which the Second Level will share with the Secretariat's senior management team ("SMT"), RMC, and the Board on a quarterly basis;

(b) Ensuring all material risks are identified, assessed, mitigated, and monitored (e.g. conducting a risk control self-assessment);[4]

(c) Proposing and implementing control enhancements, in line with the GCF Risk Appetite Statement;

(d) Reporting on monitoring metrics (identified in the risk control self-assessment) to the Second Level; and

(e) Reporting each risk event to the Second Level together with a proposed assessment of impact level[5] and a proposal for changes in controls (if required).

11. IT Risks arise from all IT systems used by the GCF. The Secretariat will nominate an IT Risk Owner,[6] defined as the representative of the First Level of Responsibility for IT risks. The IT Risk Owner is responsible for the following:

(a) Providing information to the Second Level required to populate the IT Risk section of the Risk Dashboard, which the Second Level will share with the SMT, RMC and the Board on a quarterly basis;

[2] The Secretariat may choose other divisions for these processes over time. The processes themselves may also change over time.

[3] Readiness includes National Adaptation Plans; PPF: Project Preparation Facility.

[4] Risk Control Self-Assessment ("RCSA") as described in the Secretariat's internal controls manual (under development).

[5] The impact levels "Low", "Somewhat non-disruptive", "Somewhat disruptive" and "High" have been defined in GCF's Risk Register.

[6] The IT Risk Owner will likely belong to Information and Communications Technology ("ICT") within Division of Support Services ("DSS"), and will likely be nominated by the Head of ICT.

(b) Ensuring all material risks are identified, assessed, mitigated, and monitored (e.g. conducting a risk control self-assessment);

(c) Proposing and implementing control enhancements, in line with the GCF Risk Appetite Statement;

(d) Reporting on monitoring metrics (identified in the risk control self-assessment) to the Second Level; and

(e) Reporting each risk event to the Second Level together with a proposed assessment of impact level and a proposal for changes in controls (if required).

12. A risk control self-assessment must be conducted annually for high priority processes and at least once in three years for lower priority processes.

13. The Second Level of Responsibility for Operational Process Error Risk and IT Risk is the ORMC, which has the following responsibilities:

(a) Reviewing the Risk Dashboard results for Operational Risk and IT Risk;

(b) Prioritizing processes (annually) on which risk control self-assessments are conducted, and selecting the risk events posing the highest risk levels for further mitigation;

(c) Reviewing and confirming risk control self-assessment outputs, and the proposed control enhancements;

(d) Finalizing the impact level of risk events and reporting "High" and "Somewhat disruptive" impact events to the Office of the Executive Director ("OED") together with recommendations for further action;

(e) Advising the SMT, OED and RMC on key risks, the effectiveness of mitigants and controls, and alignment of residual risks with the Risk Appetite; and

(f) The Second Level will develop a recommendation, independent of the First Level, on any action required for improving the GCF's Operational Process Error Risk and IT Risk management and strengthening its adherence to the Risk Appetite Statement. This recommendation will be discussed with the First Level, reviewed and finalized with the OED.

14. The Third Level of Responsibility for Operational Process Error Risk and IT Risk is the Office of the Internal Auditor ("OIA").

IV. Business Continuity Management

15. The Heads of all GCF divisions are responsible for reporting to the ORMC and OED without undue delay, after they become aware of it, any risk event covered by this policy that threatens the safety and security of the GCF's overall operations.

16. The OED serves as the crisis director with the authority to confirm that the risk event occurring should be classified as a business disruption event and decide on the necessary measures and response plan upon the occurrence of that event.

17. The OED will notify all units of the GCF immediately upon occurrence and confirmation of a business disruption event. The ORMC will immediately report the business disruption event to the RMC. The crisis director is supported by a security task force, which shall be established by the Executive Director.

18. The security task force is responsible for developing and testing the business continuity plans to be executed upon occurrence of a business disruption event, and establishing a remote work model for the GCF operations during disruptions events.

V. Reputation Risk Management

19. Reputation Risk refers to the risk of adverse public perception which has a material effect on the credibility of the GCF.

20. Reputation Risk arises from not only GCF's activities, but also the public perception that may follow breaches in tolerance levels for all other risk types specified in the GCF Risk Register.

21. The Secretariat and the Independent Units of the GCF will jointly develop Protocols for identifying, managing and mitigating Reputational Risks arising out of or related to the implementation of the mandates of the Independent Units.

22. The Secretariat will nominate a Reputation Risk Owner. The Reputation Risk Owner is responsible for the following:

(a) Providing information to the Second Level required to populate the Reputation Risk section of the Risk Dashboard, which the Second Level will share with the SMT, RMC and the Board on a quarterly basis;

(b) Maintaining and implementing a Communications Plan that actively tries to mitigate reputation risk;

(c) Monitoring various sources of information relevant to Reputation Risk;

(d) Developing and implementing a Response Plan for high impact Reputation Risk threats (a Response Plan will be required for any reputation risk events stemming from underlying risks for which the GCF has zero risk tolerance, per the GCF Risk Appetite Statement); and

(e) Collaborating with the Second Level to ensure that when developing controls for managing risks for which the GCF has zero risk tolerance per its Risk Appetite Statement, approaches to manage reputation risk arising from such risk events are also built in.

23. The heads of all GCF divisions are responsible for reporting to the Reputation Risk Owner any threats they foresee to the GCF's reputation. These threats will be taken into account by the Reputation Risk Owner in developing the Communications Plan and any Response Plan.

24. The ORMC plays the Second Level of Responsibility role, and is responsible for the following in mitigating reputation risk:

(a) Finalizing the impact level of Reputation Risk threats, and reporting high impact events to the OED with recommendations for further action;

(b) Reviewing the Risk Dashboard results for Reputation Risk; and

(c) Reviewing and challenging the Communications Plan or Response Plan prepared by the Reputation Risk Owner from a risk perspective, and tracking the GCF's progress against the plan.

25. The Third Level of Responsibility for Reputation Risk is the Office of the Internal Auditor ("OIA").

VI. Staffing Risk Management[7]

26. Maintaining a Secretariat staff with appropriate skills and qualifications in line with the principles and guidelines set out in the Administrative Guidelines on Human Resources or any successor guidelines or policy is one of the main tenets of effective risk management at the GCF.

27. The Secretariat will nominate a Staffing Risk Owner. The Staffing Risk Owner is responsible for the following:

(a) Working with other units within the Secretariat to assess current and future staffing and skills requirements;

(b) Providing information to the Second Level required to populate the staffing risk section of the Risk Dashboard, which the Second Level will share with the SMT, RMC, and the Board on a quarterly basis;

(c) Reviewing staff complaints to identify any systematic themes;

(d) Developing succession plans; and

(e) Taking into account the relevant human resources guidelines or policies in force when dealing with matters related to staffing risk.

28. The ORMC plays the Second Level of Responsibility role, and will be responsible for:

(a) Reviewing the GCF Risk Dashboard results and succession plan; and

(b) Developing a recommendation, independent of the First Level, on any action required for improving the GCF's staffing risk management and strengthening its adherence to the Risk Appetite Statement. This recommendation will be discussed with the First Level, reviewed and finalized with the OED.

29. The Third Level of Responsibility for Staffing Risk is the Office of the Internal Auditor ("OIA").

VII. Administrative provisions

30. This Policy takes effect on 2 April 2018.

31. This policy shall be reviewed every two years, but earlier reviews and consequential revisions may occur upon recommendation by the Secretariat or following a request from the RMC or the Board. Any resulting revisions to this policy which are of a material and/or substantive nature shall be presented to the Board for its consideration and approval.

[7] This section will be reviewed when the updated Administrative Guidelines on Human Resources is approved by the Board.