Annex VIII: Compliance risk policy

I. Introduction

1. In order to uphold and commit to achieving the highest standards of integrity, ethics and transparency in the conduct and governance of all its activities as expected of an international organization, and to minimize reputational risks that GCF may encounter, a proper compliance framework is required for GCF. It should be noted that this document sets out a principles-based policy to provide guidance regarding the roles and responsibilities across major activities for the compliance risks relevant to the GCF.

2. This policy is designed to promote a culture of compliance and setting a "tone at the top"[1]. This document presents an important element of the risk management framework (RMF), the policy governing compliance risk management for GCF.

II. Objective and scope

2.1 Objective

3. The compliance risk policy (hereinafter "the policy") provides a framework to deal with compliance risks. The policy is aligned with the fit-for-purpose compliance framework (hereinafter "the compliance framework") and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) principles that were adopted by GCF.[2] This document deliberately aims to be aspirational as the underlying framework and capabilities are built in the context of GCF business.

4. This policy applies to all GCF Personnel[3], to protect GCF, and its reputation, from being misused in compliance-related incidents by ensuring they discharge their responsibilities in a manner that enables the full implementation of this policy. This policy does not apply to GCF's accredited entities (AEs), delivery partners (DPs) and/or any other external party to the GCF.

2.2 Definition and scope of compliance risk

5. Compliance risk for the GCF arises because the following may occur:

(a) Internal compliance breaches as set out in risk code 1.1 of the risk register adopted pursuant to decision B.17/11;[4]

(b) External compliance breaches as set out in risk code 1.2 of the risk register adopted pursuant to decision B.17/11; and

(c) Inappropriate investment activities and violation of fiduciary duty.

[1] Defined as the commitment of the board and senior managerial levels of an organization towards openness, honesty, integrity, and ethical behaviour.
[2] Decision B.BM-2015/06.
[3] GCF Personnel means (i) all persons appointed to a post in the GCF under a letter of appointment, and (ii) any other individual contracted and/or engaged by the GCF to perform official functions for the GCF.
[4] This policy shall not apply to policies set out in risk code 1.1 to the extent that such policies have their own control and remedial frameworks built into such policies.

6. To further detail the compliance risks and fully define the scope, the Secretariat shall develop a list of relevant compliance risk events[5] with responsible control oversight functions assigned within the Secretariat. The comprehensive list of the compliance risk events and assigned control oversight functions are outlined in the compliance risk categorization overview.

2.3 Guiding principles

7. The GCF compliance framework has the objectives of establishing and maintaining effective GCF-wide compliance risk management. Taking into consideration the fact that GCF is an evolving and growing organization, policy design is based on the principle of establishing a risk-based ex ante approach defining controls and monitoring commensurate to the expected impact and likelihood of occurrence of a compliance risk event.[6]

8. The following provides guidance on the three levels of responsibilities in managing compliance risk:

(i) **First Level of Responsibility (First Level)**: the First Level of compliance risk management and control is with the accountable units, who are the primary owners and managers of compliance risk as part of their standard business operations. The First Level functions lie within the Secretariat and shall be designated in accordance with paragraph 12;

(ii) **Second Level of Responsibility (Second Level)**: the Second Level is independent from the First Level and ensures risks are appropriately managed given the asymmetric incentives, short-termism and optimism of risk takers. The Second Level is also known as the control oversight function. Second Level responsibilities lie within the Secretariat and shall be designated in accordance with paragraph 12; and

(iii) **Third Level of Responsibility (Third Level)**: the Third Level focuses on the independent review, assurance and accountability of the actions and interactions of the First and Second Levels, and of the compliance framework for potential deviations from its original intentions. The Third Level will develop and perform audits, reviews and other 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 risks of GCF appropriately. Third Level responsibilities rest with the Office of the Internal Auditor, the Independent Evaluation Unit (IEU), the Independent Redress Mechanism (IRM) and the Independent Integrity Unit (IIU) within the scope of their respective terms of reference (TOR).

9. In the event of any inconsistency between this policy and the TORs of the independent units, the TORs of the independent units shall prevail.

10. The First and Second Levels shall collaborate with the Third Level and provide timely information which the Third Level determines to be necessary to facilitate the implementation of its respective responsibilities under this policy.

[5] Compliance risk events refer to the incident that occurs as a result of a breach in a compliance risk.

[6] Further definition of expected impact and likelihood of occurrence to be included in the compliance risk assessment manual (an internal manual on conducting the compliance risk assessment developed by the compliance function for the Secretariat).

11. To ensure that the three levels have non-conflicting interests and are independent of each other, none of the divisions or units may be assigned overlapping responsibilities for the same process.

12. The Executive Director shall designate the First and Second Level functions and responsibilities based on the results of the compliance risk assessment.

III. Definition of terms

13. The following are definitions of the key terms applicable for this policy:

(a) **Compliance framework:**

(i) The compliance framework is an overarching framework comprising the compliance-related components necessary to operationalize an effective compliance risk management practice in GCF; and

(ii) The compliance framework shall include the following elements:

(1) **Compliance risk categorization overview**: outlines all types of compliance risk events that are potentially in scope for GCF and will continue to evolve over time as a growing document;

(2) **Compliance risk assessment manual**: outlines the detailed process of the compliance risk assessment that ensures a risk-based approach to managing compliance risks at GCF; and

(3) **Gap analysis of compliance-related policies:** outlines relevant internal policies in place to manage compliance risk events at GCF.

(b) **Compliance function:** There shall be designated within the Secretariat a compliance function, whose responsibilities, in addition to those set out in this policy, shall be determined by the Executive Director.

(c) Control oversight function:

(i) The control oversight function is the Second Level within the three levels of responsibilities framework for compliance risk. It is responsible for supporting the First Level in identifying, assessing, mitigating and monitoring compliance risk events; and

(ii) The control oversight responsibility is designated to the most appropriate function identified as an outcome of the compliance risk assessment;[7]

(d) Investment-related and administrative business process:

(i) The controls management process within the policy is structured based on the key investment-related and administrative business processes of GCF;

(ii) The key investment-related processes[8] include:

(1) Accreditation and entity relationship management;

[7] The compliance risk assessment involves preparing a comprehensive list of all relevant compliance risk events to be assessed for their respective risk levels. This assessment is then reviewed by the compliance function, upon which mitigation actions and controls can be assigned to effectively mitigate the risk.

[8] Please note the list of investment-related business processes is not exhaustive and is subject to developments.

(2) Readiness and preparatory support, including national adaptation planning, (hereinafter "readiness") and Project Preparation Facility (PPF) proposals, concept notes and funded activity proposal reviews;

(3) Disbursements for all funding requests;

(4) Readiness, PPF and funded activity monitoring; and

(5) New financial instrument development.

(iii) The key administrative business processes[9] include:

(1) Procurement;

(2) Contract handling;

(3) Data handling;

(4) Personnel recruitment and management; and

(5) Knowledge management.

IV. Managing compliance risks

14. To ensure effectiveness and efficiency in carrying out activities necessary to manage the compliance risks referred to in paragraph 5, the Second Level shall have:

(a) The authority to request and receive all relevant and necessary documents and paper or electronic data from the First Level; and

(b) The right to provide compliance considerations to be factored into relevant business decisions.

15. Furthermore, the Heads of each designated First Level division and/or unit have the authority to perform the aforementioned tasks (i.e. paragraphs 14 (a) and (b)) for their respective personnel.

V. Roles and responsibilities – compliance risk management

16. The roles and responsibilities for compliance risk management are based on the following key functional compliance activities:

(a) Risk identification;

(b) Risk assessment;

(c) Controls management (investment-related business processes, administrative business processes);

(d) Monitoring and reporting;

(e) Risk mitigation;

(f) Training and communication.

17. In addition, IEU – in its Third Level capacity within the context of this policy – may, upon request, provide to the Board and Senior Management of the Secretariat assessments and evaluation reports of the effectiveness and efficiency of risks identified, assessed and mitigated.

[9] Please note the list of administrative business processes is not exhaustive.

5.1 Risk identification

18. The First Level shall work with the Second Level to define its key business processes and subprocesses, identify current and potential compliance risk events, and map them into compliance risk categories as a part of the annual[10] compliance risk assessment[11] and in alignment with the risk control self-assessment.[12]

19. The compliance function shall maintain the list of compliance risk events in its compliance risk categorization overview (which forms part of the compliance framework) and work with the First and Second Levels to update the compliance risk categorization overview on a regular basis.

5.2 Risk assessment

20. The First Level shall conduct the compliance risk assessment in close consultation with the relevant Second Level to assess the impact and likelihood of occurrence.[13]

21. The Second Level shall provide oversight of and guidance to the First Level's compliance risk assessment process, ensuring consistent application of the compliance framework, and check the First Level's risk assessment results for quality assurance.

22. The compliance function shall consolidate the results of the compliance risk assessment into the overall compliance risk matrix[14] of GCF.

5.3 Controls management – investment-related business processes

5.3.1 First Level – accreditation and entity relationship management

23. The First Level shall collect information, including, where available, written policies or descriptions on the internal controls management practices of each AE with regard to relevant checks under applicable internal policies to ensure appropriate compliance risk management for all relevant compliance risk events as outlined in the compliance risk categorization overview.

24. When applicable, the First Level shall regularly request each AE to provide a self-assessment of its compliance with the GCF accreditation requirements, 15 in accordance with the accreditation framework for AEs.

25. The First Level, in conjunction with the relevant Second Level function(s), where applicable, shall define and maintain controls for compliance risk events based on compliance risk assessment results to ensure compliance with internal policies. In addition, the First Level shall implement the defined controls, report the results of implementation to the Second Level and be responsible for collecting data and information necessary to implement these controls.

[10] The timing and process for the compliance risk assessment may be subject to change during the initial set-up phase.
[11] Details on processes and procedures to be included in the compliance risk assessment manual.
[12] Details on processes and procedures to be included in the internal controls manual (part of the GCF risk management framework).
[13] Definitions on impact and likelihood of risk to be included in the compliance risk assessment manual.
[14] The compliance risk matrix summarizes the compliance risk assessment across all compliance risk events.
[15] Some accreditation master agreements may not have this requirement.

5.3.2 First Level – review of readiness and preparatory support, including national adaptation planning, and Project Preparation Facility proposals, concept notes and funded activity proposals

26. The First Level shall:

(a) Define and maintain controls for compliance risk events with regard to the development and review of readiness and PPF proposals;

(b) Define and maintain controls for compliance risk events with regard to the development and review of concept notes and funded activity proposals;[16]

(c) Perform these functions, in conjunction with the Second Level, based on the results of the compliance risk assessment and any other assessment[17] to ensure compliance with the investment framework, fiduciary standards and other GCF internal policies;

(d) Implement the defined controls and report the results of implementation to the Second Level; and

(e) Be responsible for collecting the relevant data and information necessary to implement these controls.

5.3.3 First Level – first disbursements

27. The First Level, in conjunction with the relevant Second Level function, shall define and maintain controls for compliance risk events with regard to the first disbursement of funds based on the compliance risk assessment results and compliance with the accreditation master agreement (AMA), funded activity agreement (FAA) and readiness/PPF grant agreements. In addition, the First Level shall implement the defined controls, report the results of implementation to the Second Level and be responsible for collecting the relevant data and information necessary to implement these controls.

5.3.4 First Level – readiness, Project Preparation Facility, and funded activity monitoring and subsequent disbursements

28. The First Level, in conjunction with the Second Level, shall define and maintain controls for compliance risk events with regard to the monitoring of readiness, PPF, and funded activities and subsequent disbursements based on the compliance risk assessment to ensure compliance with the AMA, FAA, readiness and/or PPF grant agreements, as appropriate. In addition, the First Level shall implement the defined controls and report the results of implementation to the Second Level, and be responsible for collecting data and information necessary to implement these controls.

5.3.5 Second Level – investment-related business processes

29. The Second Level shall be responsible for the following activities:

(a) Providing support in the definition of controls to the First Level;

(b) Monitoring and tracking progress of controls implementation;

[16] This includes proposals submitted through request for proposal, simplified approval process and enhanced direct access.

[17] For readiness and Project Preparation Facility proposals, this includes results from the financial management capacity assessment.

(c) Providing input on the data and information supporting the implementation of controls for the process, as collected by the First Level; and

(d) Reporting critical control insufficiencies to the compliance function.

5.4 Controls management – administrative business processes

30. The First Level, in conjunction with the Second Level, shall define and maintain controls for compliance risk events with regard to the administrative business processes for GCF, based on the compliance risk assessment results, to ensure compliance with relevant policies. In addition, the First Level shall implement the defined controls, report the results of implementation to the Second Level, and be responsible for collecting the relevant data and information necessary to implement these controls.

31. The Second Level shall be responsible for the following activities:

(a) Providing support in the definition of controls to the First Level;

(b) Monitoring and tracking progress of controls implementation;

(c) Providing input on the data and information supporting the implementation of controls for the process, as collected by the First Level; and

(d) Reporting critical control insufficiencies to the compliance function.

5.5 Monitoring and reporting

32. The First Level shall receive data input on compliance breaches, claims, investigations or proceedings commenced on the funded activity from AEs, in accordance with the relevant legal agreements, and will provide necessary data input to the Second Level for periodic reporting, including data input required to monitor compliance key risk indicators, which are the main risk metrics to be tracked by GCF as defined by the Second Level as part of the compliance risk assessment.[18]

33. The First Level will regularly monitor compliance with current readiness, PPF and funded activities through necessary reports provided by the AE, in accordance with the relevant legal agreements, and inform the Second Level, as required, of any compliance breaches, non-compliance or potential risk events. Furthermore, the First Level will inform IIU of compliance breaches, non-compliance and potential risk events within any of the integrity policies or standards of the GCF.

34. The Second Level will also review compliance-related issues raised by the First Level, and execute follow-up actions as necessary, receiving support from the compliance function or the IIU as needed and in accordance with GCF policies and procedures and in line with the relevant legal agreements.

35. The compliance function shall compile and monitor compliance key risk indicators defined by the Second Level, review periodic compliance reports as well as any notifications of compliance breaches and recommend actions if required.

36. The compliance function will report material compliance breaches or events to the Head of the Office of Risk Management and Compliance (ORMC), the Office of the Executive Director

[18] Details on processes and procedures to be included in the compliance risk assessment manual.

(OED)[19] and the Risk Management Committee (RMC), except for areas related to AML/CFT and other prohibited practices.[20] The compliance function shall further report any information or allegations of integrity violations to the IIU immediately upon becoming aware of them and shall seek advice from the IIU in determining mitigation actions where red flags have been identified.

37. Upon request by the Board or SMT, the IEU – in line with its annual workplan – will evaluate and assess any risks identified and the implementation of the control and mitigation activities undertaken in turn by the First and Second Levels.

5.6 Risk mitigation[21]

38. When a compliance breach occurs, the First Level, with support from the Second Level, shall develop and implement risk mitigation actions, either developed through the compliance risk assessment or, if a new compliance risk event occurs, developed on an ad hoc basis.

39. The Second Level shall provide advice on the development of compliance risk mitigation actions, including new controls, improved controls and strengthened monitoring, to the First Level. The Second Level shall analyse risk alerts when received and ensure that appropriate compliance risk mitigation action is taken, track progress of the implementation of compliance risk mitigation actions, and regularly inform the compliance function of the progress of the compliance risk mitigation actions.

40. In accordance with the relevant legal agreements, for compliance risk events triggered by readiness, PPF or funded activities, the relevant contractual counterparties are responsible for carrying out necessary risk mitigation actions. The First Level shall be responsible for liaising with the AE or delivery partner to monitor risk mitigation actions. When deemed necessary, GCF will intervene and execute further risk mitigation actions. The risk mitigation actions shall be performed in accordance with the AMA, FAA and readiness and/or PPF grant agreements, as appropriate.

41. Upon becoming aware of credible risk of integrity violations as defined in the TOR for the IIU, GCF Personnel shall immediately inform IIU.

5.7 Training and communication

5.7.1 Compliance training

42. The compliance function shall be responsible for the following activities:

(a) Delivering training on compliance-related due diligence on a regular basis in person in order to enable the First and Second Levels to discharge their responsibilities under this Policy, through eLearning course modules and additional ad hoc, incident-based training sessions as necessary to GCF;

(b) Developing and maintaining, in conjunction with Second Level functions, compliance training toolkits and curricula complete with the training format, frequency and personnel, which is approved by OED;

[19] The compliance function will report directly to the Office of the Executive Director when the breach involves the Head of ORMC.

[20] These will be reported to the Ethics and Audit Committee or the Independent Integrity Unit in accordance with applicable Board policies, depending on the breach committed.

[21] These provisions shall not apply to processes set out in risk code 1.1 to the extent that such processes have their own control and remedial frameworks built into other policies.

(c) Ensuring alignment, in conjunction with the other Second Level functions, in respect of shared tools, processes and expert knowledge; and

(d) Improving compliance training programmes based on feedback gathered from the First and Second Levels.

43. Human Resources and Procurement within the Division of Support Services shall maintain training history records for all GCF Personnel, as reported by the Head of each division and unit.

44. The Secretariat must stay up-to-date on the latest compliance training curriculum.

45. The Head of each designated division and/or unit shall be accountable for ensuring that covered individuals complete the required training programmes.

5.7.2 Internal and external communication

46. The Secretariat shall promote awareness and encourage compliance through regular communication with GCF Personnel and external parties.

47. The Secretariat will develop and maintain both internal and external communication plans for crisis situations as a part of its communications plan and any response plan. The details of roles and responsibilities for communications on non-compliance and compliance-related reputational risks will be outlined in the communications plan and any response plan.

VI. Administrative provisions

48. The Secretariat will develop an implementation plan for this policy. This policy will take effect on 2 September 2019.

49. This policy shall be reviewed by the compliance function 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.