United Nations Development Programme
POLICY ON ENTERPRISE RISK MANAGEMENT
January 2016
# Table of content

1 Objectives................................................................................................................................. 2

2 Terms and Definitions.................................................................................................................. 2

3 ERM Process.................................................................................................................................. 3

  3.1 Establishing the context............................................................................................................. 3

  3.2 Risk Assessment....................................................................................................................... 3

  3.3 Risk Treatment.......................................................................................................................... 5

  3.4 Monitoring and Review............................................................................................................ 6

  3.5 Communication and consultation............................................................................................. 6

4 Roles and Responsibilities............................................................................................................. 6

  4.1 Line Management...................................................................................................................... 7

  4.2 Risk Committee......................................................................................................................... 7

5 Appendices..................................................................................................................................... 9
1 Objectives

1. UNDP is exposed to a variety of external and internal influencing factors that create uncertainty regarding the realization of organizational goals. The effect of this uncertainty on the objectives is also referred to as “risk”. UNDP’s Enterprise Risk Management (ERM) System allows UNDP to manage these risks and

- identify and treat risk throughout the organization,
- identify opportunities and threats,
- encourage proactive management and better informed strategic decision taking and
- effectively allocate and use resources for risk treatment.

This will enable the organization to

- secure life and property,
- support the effective achievement of results,
- safeguard the accountable use of resources and
- protect corporate reputation.

2 Terms and Definitions

Business process. A Business process is the set of activities supporting an organizational structure in achieving its objectives.

Consequence. The outcome of an event affecting objectives. An event can lead to a range of consequences, and initial consequences can escalate through knock-on effects. A consequence can be certain or uncertain, can be expressed qualitatively or quantitatively, and can have positive or negative effects on objectives.

Event. The occurrence or change of a particular set of circumstances. An event can be one or more occurrences, can have several causes, and can consist of something not happening. An event is sometimes referred to as an “incident” or “accident”.

Likelihood. The chance of something happening. The equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Likelihood signals that the chance can be described in both general terms and mathematically.

Risk. The effects of uncertainty on organizational objectives. An effect is a deviation from the expected — positive and/or negative. It is best practice to formulate risk in the term of “future event”.

Risk assessment. The overall process of risk identification, risk analysis and risk evaluation.

Risk level. Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.

Risk management. Coordinated activities to direct and control an organization with regard to risk.

Risk manager. A designated person responsible for facilitating and coordinating the management of risk.

Risk owner. The person or entity with the responsibility to manage a risk.
**Risk profile.** A description of any set of risks. The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

**Risk register.** A risk management tool that serves as record of all risk identified by the unit. For each risk identified, it should include information such as likelihood, consequences, treatment options, etc. (please see template risk register).

**Risk treatment.** A measure to modify risk exposure to provide reasonable assurance towards the achievement of objectives.

---

**3 ERM Process**

3. UNDP’s ERM Process is largely based on ISO’s Internal Risk Management Standard (ISO 31000). It consists of the following steps:

3.1 Establishing the context

4. UNDP’s risk management methodology is applied at all organizational levels within its relevant internal and external context. This includes corporate wide elements such as the organization’s strategic objectives but also the country office specific context (e.g. the particular group of stakeholders a unit interacts with). Establishing the context allows for the identification of risks that are relevant to the organization and a contextualized application of all subsequent elements of the ERM process.

3.2 Risk Assessment

5. Risk assessment is the overall process of risk **identification**, risk **analysis**, risk **evaluation** and risk **reporting**. When assessing risks throughout the organization, the criteria model is used as it sets out how UNDP measures risk.

Risk **identification:**

6. Identify risks relevant to the established context and the organizational objectives, where each risk consists of three components; event, cause, and impact. A list of critical risks is generated that might enhance, prevent, degrade, accelerate or delay the achievement of the objectives.

Risk **analysis**

7. Assign a likelihood and consequences of the risk by applying the criteria model. By considering causes and existing controls, the likelihood and consequences of a risk are estimated. Where applicable, in place of the criteria model, the use of more detailed analytical tools are also encouraged (e.g. security risk analysis, social and environmental impact assessment).

Risk **evaluation**

9. Take decisions based on the outcome of the risk analysis. The risk levels of all analyzed risks are evaluated to determine which risks need treatment and their priority.
Risk acceptance

10. Risk acceptance defines the level of risk that UNDP is willing to accept in order to meet its objectives. When an assessed risk exceeds the acceptable risk level, management of the risk must be initiated.

<table>
<thead>
<tr>
<th>General Acceptance Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Red:</strong> The risk requires immediate action. If an appropriate treatment cannot be initiated stop ongoing activities. Risk should be reported to superior.</td>
</tr>
<tr>
<td><strong>Orange:</strong> The risk requires prompt action. While activities can be continued, initiate treatment and report to superior as soon as possible.</td>
</tr>
<tr>
<td><strong>Yellow:</strong> The risk requires treatment. Initiate treatment within the allowable time frame.</td>
</tr>
<tr>
<td><strong>Green:</strong> The risk is acceptable and does not require treatment. Monitor.</td>
</tr>
</tbody>
</table>

11. UNDP might have different risk appetite for different categories of risk, in that regard, the risk acceptance guidance would be provided by the respective office (e.g. security office for security risks, OFRM for financial risks, and BPPS for programming related risks) for decision making.

Risk reporting

12. Reporting of risks is an inherent part of the risk assessment process. The reporting of risks and risk profiles helps UNDP to create risk awareness at all levels of the organization, and ultimately builds a transparent and improved decision making process.

At the corporate level, the main body tasked with analyzing and reporting the overall risk profile of UNDP is the Risk Committee. The Risk Committee is a subcommittee of the Executive Group (EG) and reports to the EG on a quarterly basis. It should keep the EG informed on deliberations, including emerging, escalated or increasing corporate risks and propose risk mitigation strategies when needed.

Similarly, all other organizational offices should regularly report risks and risk profiles to the next level of management (see “Roles and Responsibilities” for more information).

13. The following reports are required:

**Annual reporting.** All UNDP offices are required to include risk reporting in their Integrated Work Plan (IWP) and related regular annual reporting mechanism (ROAR). This includes a summary of the current risk landscape (risk matrix), a description of the overall impact of risks on the objectives for the next financial year, and a list of the top key risks and the treatment status. The annual report should be made in conjunction with the UNDP budget and business planning process. The report should be preceded by an updated risk register. The update should include a follow up of last year’s risk treatment progress, a re-assessment of risks in light of changing circumstances and/or ongoing treatments, and new risks may be added to the register.

The Risk Committee submits an annual risk report to the EG, based on a strategic analysis of UNDP’s overall risk landscape.
Quarterly monitoring/reporting. All offices are required to update the risk register on the quarterly basis. This should be an integral part of quarterly monitoring of work plans (through the IWP). When appropriate, this monitoring exercise should update the risk level and the treatment status. The updates may also include additional information as seen appropriate and important by the respective office.

At the corporate level, the Risk Committee submits a quarterly risk report to the EG, based on a strategic analysis of UNDP’s overall risk landscape. The fourth quarter report is replaced by an annual report.

Ad-hoc reporting. In addition to the quarterly and annual reports, and in line with the risk acceptance guidelines, the occurrence of “red” and “orange” risks should also be reported on an ad-hoc basis. The ad-hoc reports should include a description and assessment of the risk, the initiated treatment/status and call for action or request for assistance. If the risk has been escalated, the reason of escalation along with a suggested course of action should be included. Ad-hoc reporting may be done in any suitable and convenient way, e.g. by e-mail or phone. The risk register should be updated as soon as possible.

3.3 Risk Treatment

14. Identify one or more treatment options and implement the options considered most effective. Options may be of four types: terminate, mitigate, transfer or tolerate. All risks shall be assigned to a risk owner, who is responsible for reporting the risks and assuring that they are treated appropriately.

Risk escalation

15. As a general principle, risks should as far as possible be handled by line management (i.e., project or country office for project related risks) and treated by the Risk Owner or a person appointed by the Risk Owner. In some cases, however, circumstances pertaining to the treatment itself may exceed the authority/mandate of the Risk Owner, for example:

- treatment of the risk requires decisions/actions, e.g. expenditures, that are beyond what the risk owner is authorized to decide;
- the risk cuts across, or may impact, multiple offices (e.g. it affects a number of Country Offices or the entire organization), and/or addressing the risk requires action by multiple offices; or
- addressing the risk requires corporate changes (e.g. changes to corporate policies); or;
- grievances from stakeholders have been received to which the risk owner cannot impartially and/or effectively respond.

16. If one or more of the above conditions are met, the risk should be escalated by the Risk Owner. When a risk is escalated, the Risk Owner must provide the receiving manager with complete information about the risk in order to enable the receiving manager to act appropriately. If and when escalation is urgent, it is acceptable to communicate escalation using phone or e-mail and update the risk register afterwards.

17. When a risk is escalated and accepted the ownership of the risk is also transferred to the receiving manager, meaning that it is now his/her responsibility to take action. However, it is important to note that the change of ownership will not take place until the receiving manager has confirmed that he/she accepts the ownership. A response to the request for risk transfer should be provided latest within 5 working days. The escalation of the risk and the change of ownership should be noted in the risk register.
18. If the receiving manager decides that the risk does not warrant escalation, it may be de-escalated (to the original risk owner or other suitable person). Any de-escalation of risks should be noted in the risk register along with the accompanying change of risk ownership.

19. As a general principle, escalation should follow the applicable organizational structure i.e. from project to country office to Bureau (central/regional) and ultimately to the corporate level.

3.4 Monitoring and Review

20. Monitoring and review shall be a planned part of the risk management process and involves regular checking and/or surveillance to make sure that treatments had the intended effect. It can be periodic or ad hoc and is done to see if: further action is needed; appropriate controls are in place; new uncertainties are emerging; and strategic changes to UNDP’s risk landscape require senior management action. The results of monitoring and review should be recorded and reported as appropriate, and should also be used as an input to auditing, and reviews of the risk management framework.

3.5 Communication and Consultation

21. Communication and consultation with relevant stakeholders should take place at all stages of the risk management process and at regular/planned intervals.

4 Roles and Responsibilities

22. The ERM requires clear lines of risk ownership at all levels of the organization. For each risk, there are three levels of responsibility, namely accountability, ownership and execution.

23. The top layer of accountability follows the line hierarchy, i.e. the line manager of each unit is accountable for risk management within his/her area of responsibility. To give an example, the Director of a Regional Bureau is ultimately responsible for assuring that his/her Regional Bureau and its Country Offices on a regular basis identify, analyze and manage risks.

24. The second layer of ownership does not follow a line hierarchy by default; an owner can be anyone who has been assigned such responsibility. Usually, ownership is assigned based on the principle of who is “best suited”. A Risk Owner must be assigned to each individual risk, and as such, responsibility is typically based on who is familiar with the risk and has the skills, authority, and accountability to manage the risk.

25. The third layer of execution refers to the person that is responsible for a specific task. This can, for example, be a project member, who has been assigned the responsibility to treat a risk.

26. The same person could have all three responsibilities, e.g. a project manager is accountable for a project and could very well also be responsible for managing and treating a risk.

27. The roles and responsibilities of the ERM framework may be divided into line management and support functions, where line management is accountable for the content, such as risk assessments and
updated risk profiles; and support functions uphold and maintain the ERM system as such and carries out strategic assessment and analysis of the overall UNDP risk profile.

28. Roles and responsibilities for risk management at the Programme and Project level are clarified further in UNDP’s Programme and Project Management policies and procedures.

4.1 Line Management

29. The roles and responsibilities pertaining to the input and output of the ERM-process ultimately lies with line management at each level of the organization. In the event of a different opinion among stakeholders, the responsibility of line management shall always be prioritized. While the actual treatment of risks may be executed by other internal or external units/functions (e.g. at the project level multiple roles and responsibilities pertain to risk management), the responsibility for managing risks remains with line management:

a. Directors of Bureaux and other HQ Units

30. Are accountable for ensuring that the country office risk registers are regularly updated, the identified risks are treated and that any risk that cannot be addressed by the country office is escalated/brought to the attention of the EG through the Risk committee. Directors of Bureaux are also responsible for ensuring that offices under their supervision (e.g. Country Offices for Regional Bureau and Liaison Offices for BERA) keep their risk registers up to date, treat risks appropriately, report upwards in line as necessary.

b. Head of Office/Programme Manager

31. Is responsible for ERM at the office/programme level, accountable to the Bureaux for ensuring that the office’s Risk register is regularly updated, that risks are treated and that any risk that cannot be addressed at the Office level is escalated to the Bureau.

c. Project Managers

32. Is responsible for ERM at the project level and reports to the Project Boards in line with established practices. Further application of this policy in Project Management shall be clarified in the Project Management policies and procedures.

4.2 Risk Committee

33. The Risk Committee is established at the corporate level and is a sub-committee of the EG. The Risk Committee reports to the EG on a quarterly basis and when so requested. The Committee is chaired by the Associate Administrator with membership from UNDP Senior Management team. Other representatives, invited experts and other relevant roles may be invited to the Committee as needed. The main responsibilities of the Risk Committee are:

- Ensuring that the overall Risk framework is effective, relevant and applied corporately;
- Reviewing and analyzing the aggregated risk log (and escalated risks) on a regular basis with the purpose of identifying strategic risks and issues which require the attention of EG, developing proposals for managing escalated issues/risks (including Business Continuity Management (BCM) and Incident & Crisis Management (ICM) actions. As part of its work, the Risk Committee is responsible for preparing an annual UNDP risk report for consideration of the EG.
34. The Risk Committee should convene at least quarterly, but may also meet when requested by the EG. A full description of the roles and responsibilities of the Risk Committee can be found in Appendix 3.

35. In performing its duties, the Risk Committee is supported by an ERM Support Function at the corporate level, which is responsible for keeping the ERM documentation relevant and up to date. It is also responsible for the risk register and for aggregating and analyzing risk profiles and producing corporate-wide risk reports that are presented to the Risk Committee.
## Appendices

### Appendix I: Risk Categories

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Human rights violations</td>
<td>2.1 External factors</td>
<td>3.1 Complex design</td>
<td>4.1 Institutional arrangements</td>
<td>5.1 Corruption</td>
<td>6.1 New unexpected regulations, policies</td>
<td>7.1 Partnership failing to deliver</td>
</tr>
<tr>
<td>2.2 Gender discrimination</td>
<td>2.2 Internal factors</td>
<td>3.2 Project management</td>
<td>4.2 Institutional/execution capacity</td>
<td>5.2 Government commitment</td>
<td>6.2 Critical policies or legislation fails to pass or progress in the legislative process</td>
<td>7.2 Strategic vision, planning &amp; communication</td>
</tr>
<tr>
<td>1.3 Loss of biodiversity and unsustainable use of natural resources</td>
<td>2.3 Human error/incompetence</td>
<td>3.3 Human error/incompetence</td>
<td>4.3 Implementation arrangements</td>
<td>5.3 Political will</td>
<td>7.3 Leadership &amp; management</td>
<td></td>
</tr>
<tr>
<td>1.4 Climate change</td>
<td>2.3 Human error/incompetence</td>
<td>3.4 Infrastructure failure</td>
<td>4.4 Country office capacity</td>
<td>5.4 Political instability</td>
<td>7.4 Programme alignment</td>
<td></td>
</tr>
<tr>
<td>1.5 Community health and safety (including natural disasters)</td>
<td>2.5 Safety being compromised</td>
<td>3.5 Safety being compromised</td>
<td>4.5 Governance</td>
<td>5.5 Change in government</td>
<td>7.5 Competition</td>
<td></td>
</tr>
<tr>
<td>1.6 Working conditions</td>
<td>2.6 Poor monitoring and evaluation</td>
<td>3.6 Poor monitoring and evaluation</td>
<td>4.6 Culture, code of conduct &amp; ethics</td>
<td>5.6 Armed conflict and instability</td>
<td>7.6 Stakeholder relations</td>
<td></td>
</tr>
<tr>
<td>1.7 Cultural heritage</td>
<td>2.7 Delivery</td>
<td>3.7 Delivery</td>
<td>4.7 Accountability &amp; compensation</td>
<td>5.7 Adverse public opinion/media intervention</td>
<td>7.7 Reputation</td>
<td></td>
</tr>
<tr>
<td>1.8 Displacement and resettlement</td>
<td>2.8 Programme management</td>
<td>3.8 Programme management</td>
<td>4.8 Succession planning &amp; talent management</td>
<td>7.8 UN coordination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.9 Indigenous people</td>
<td>2.9 Process efficiency</td>
<td>3.9 Process efficiency</td>
<td>4.9 HR processes &amp; procedures</td>
<td>7.9 UN reform</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.10 Pollution and waste</td>
<td>3.10 Internal controls</td>
<td>3.10 Internal controls</td>
<td>3.10 Internal and external fraud audit</td>
<td>3.11 Compliance and legal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.11 Compliance and legal</td>
<td>3.12 Compliance and legal</td>
<td>3.13 Procurement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.13 Procurement</td>
<td>3.14 Technology</td>
<td>3.14 Technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.14 Technology</td>
<td>3.15 Physical assets</td>
<td>3.15 Physical assets</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appendix: II Criteria Model

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>not likely</th>
<th>moderately likely</th>
<th>Likely</th>
<th>Highly likely</th>
<th>Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Every 5 years or less or very low chance (&gt;20%) of materializing</td>
<td>Every 3-5 years or low chance (20% - 40%) of materializing</td>
<td>Every 1-3 years or chance of materializing between 40% - 60%</td>
<td>Once or twice a year or high chance of materializing (60% - 80%)</td>
<td>Several times a year or chance of materializing above 80%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Low 1</th>
<th>Moderate 2</th>
<th>High 3</th>
<th>Significant 4</th>
<th>Critical 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety &amp; Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Likelihood

- **Not likely**: Every 5 years or less or very low chance (>20%) of materializing.
- **Moderately likely**: Every 3-5 years or low chance (20% - 40%) of materializing.
- **Likely**: Every 1-3 years or chance of materializing between 40% - 60%.
- **Highly likely**: Once or twice a year or high chance of materializing (60% - 80%).
- **Expected**: Several times a year or chance of materializing above 80%.

### Consequence

<table>
<thead>
<tr>
<th>Description of consequence</th>
<th>Low 1</th>
<th>Moderate 2</th>
<th>High 3</th>
<th>Significant 4</th>
<th>Critical 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety &amp; Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial (absolute and relative)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Expected range in USD, 3 numbers:**
- **Maximum (worst case)**
- **Likely (best guess)**
- **Minimum (best case)**

which, based on best guess figure, corresponds to:

- <5% of applicable budget
- 5-20% of applicable budget
- 20-30% of applicable budget
- 30-50% of applicable budget
- >50% of applicable budget

More than 50% of the applicable and planned results/outcome affected and/or in jeopardy

Risk of permanent disruption in applicable operations

Major deviation from applicable rules and regulations

Multiple casualties among UNDP staff or partners and/or loss of life to general population directly or indirectly caused by UNDP actions

Negative reports/articles in several national, regional and/or international media for a period of a week or more, and/or criticism from key stakeholders

Negative reports/articles in several national, regional and/or international media for a period of a month or more, and/or strong criticism from key stakeholders
Appendix III: ToR Risk Committee

Background

Enterprise risk management (ERM), including the strategic aspect of incident & crisis management (ICM), are all integral parts of Risk, and disciplines of effective managing for development results. As UNDP moves towards programmes involving higher level of policy advice and system-wide transformational change, the achievement of programmatic results will increasingly depend on factors fully or partially beyond our control. These include risks which we must navigate and manage in cooperation with partners and other stakeholders. Capitalizing on promising opportunities often requires the organization to take calculated risks. Being agile, responsive, and proactive is critical to our achievement of results.

UNDP’s Risk management framework will guide the conduct and application of ERM and defines roles and responsibilities. At the corporate level, a Risk Committee is chaired by the Associate Administrator to oversee the overall implementation, and use, of the framework in UNDP. The Risk Committee is a subcommittee of the EG and reports back to the EG on the framework on a quarterly basis.

Duties and Responsibilities

In line with the relevant policy(ies), the Risk Committee is responsible for:

1. Reviewing and analyzing Corporate risks
   Under this responsibility, the committee will review, and deliberate risk management strategies and where necessary, proposed amendments or revised strategies. The committee shall focus on strategic corporate risks that are escalated to the committee, while leaving the operational risks discussion in other respective forums. (e.g the OPG, SMG, ET and Crisis board).

   a. Corporately identified risks;
      The chair and the member of the committee can bring to the table risks that are identified and need to be escalated to the committee through the different corporate mechanisms, e.g:
      - The Organizational Performance Group (OPG) for significant institutional risks related to the organizational performance, including the top audit risks priorities;
      - The Executive Team, for risks related to context and environments where specific country office is operating;
      - The Crisis board, for risks related to a particular country programme in on-going crisis;
      - The Security Management Group for risks related to staff safety and security as well as business continuity in Headquarter; and
      Other corporate mechanisms as relevant.

   b. Analysis from aggregated risk logs;
      On a quarterly basis, risks analysis from all risks entries in the aggregated risk logs should be presented to the committee to scan for possible emerging risks and/or risks with increasing criticality that might require corporate level treatments. This analysis, when applicable might include the comparison between risks that are logged in the system and risks that materialized within the reporting period.

   c. Escalated risks from bureaux and offices
In line with the procedures for risk escalation, all risks that are escalated to the corporate level will be deliberated in the committee meeting for decisions and action points.

2. **Maintaining the overall Risk and Resilience framework**
   Under this responsibility, the committee will review Policies and Procedures related to Enterprise Risk Management, including the strategic aspects of Business Continuity Management (BCM) and Incident and Crisis Management (ICM).

   As part of this function, the committee should also look into the overall knowledge management aspect of risks, including capturing, reviewing lessons learnt and best practices to be apply and/or disseminated across the organization.

   In discharging this function, the committee might request the Organizational Performance Group (OPG) to provide inputs and comments before the policy is proposed to the Executive Group (EG) for endorsement.

Management Arrangement:

The committee is a sub-committee to the Executive Group (EG) and serves as the main platform to identify, assess, develop treatment and monitor risks at the corporate level. The committee report back to the EG on a quarterly basis.

1. **Membership of the Committee**
   The membership of the Risk Committee shall include adequate representation of corporate perspective on the five risk consequences categories (i.e. Financial and resourcing; Safety and Security; Programmatic Delivery; Institutional Effectiveness; and Reputational). In that regards, the permanent membership of the committee is as follow:

   - The Associate Administrator as chair;
   - Executive Office;
   - Director of Regional Bureau (on annual rotational basis)
   - Director of the Bureau of Management;
   - Director of BERA
   - Director of BPPS
   - Director of CRU;
   - Chief Finance Officer;

   The membership to this committee is non-substitutable. In the event that a committee member is not available to attend a risk committee meeting, the participation cannot be delegated to other staff. On an ad-hoc basis, the committee might invite other staff to sit in the risk committee meeting to deliberate on specific issues. This might include:

   - Risk owner of specific corporate risk entries;
   - Line manager of specific bureau/unit;
   - Expert or resource persons on a particular issues;
   - Other staff as necessary.

2. **Relationship with other corporate decision making structures:**
The risk committee is a sub-committee to the Executive group. It provide reports to the EG on quarterly basis and/or as needed. The relationship with other corporate decision making structures can be depicted as follow:

The risks committee review, analyses and make decisions about risks that are identified through the different corporate mechanisms (e.g. OPG, ET, SMG and Crisis Board). Decision on risks treatments should then be recommended back to the existing mechanism for implementation. The Risk Committee will monitor the status of the implementation of these treatments during the periodical risk committee meetings.

3. **Risk committee meetings:**

The risk committee shall meet on quarterly basis, preferably during the week when the EG meeting is scheduled but before the EG meeting take place. On and *ad-hoc* basis, the chair of risk committee can also call for a committee meeting for immediate deliberation of an urgent risk issues. The standing agenda for the committee meeting are as follow:

- Review the effectiveness of the ERM implementation (including the policies, procedures, learning and other tools);
- Review of the Executive Team decisions and mechanisms;
• Review of the aggregated risk logs;
• Review of the corporate risk log (including monitoring of the risk treatments);
• Any other business

4. Risk committee secretariat:

The risk committee is supported by a secretariat to assist the chair and committee members in effective and efficient management of committee meetings. This includes:
• Preparing agenda and background materials for committee meetings;
• Conduct the analysis of aggregated risk logs;
• Record and present escalated risks for committee deliberations;
• Ensure proper documentation of risk committee decisions; and
• Any other tasks as assigned by the chair of the committee.