

**UNDP Enterprise Risk Management (ERM)**

**Policy and Procedures**

**Policy Owner: BMS/BPPS**

Table of Contents

[1. Policy Scope and Objectives 1](#_Toc155179133)

[2. ERM Methodology 3](#_Toc155179134)

[2.1 Risk Communication and Consultation 3](#_Toc155179135)

[2.2 Establishing the Scope, Context and Criteria 3](#_Toc155179136)

[2.3 Risk Assessment 4](#_Toc155179137)

[Risk Identification 4](#_Toc155179138)

[Risk Analysis 4](#_Toc155179139)

[Risk Evaluation 5](#_Toc155179140)

[2.4 Risk Treatment 5](#_Toc155179141)

[Risk Treatment Options 5](#_Toc155179142)

[Risk Ownership and Escalation 6](#_Toc155179143)

[2.5 Risk Monitoring and Review 6](#_Toc155179144)

[2.6 Recording and Reporting 7](#_Toc155179145)

[3. ERM System 8](#_Toc155179146)

[4. Governance 8](#_Toc155179147)

[4.1 Three Lines of Defense 8](#_Toc155179148)

[First Line of Defense 8](#_Toc155179149)

[Second Line of Defense 9](#_Toc155179150)

[Third Line of Defense 10](#_Toc155179151)

[5. Risk Management Culture 10](#_Toc155179152)

[Appendix 1. Terms and Definitions 12](#_Toc155179153)

[Appendix 2. ERM Risk Categories and Sub-Categories 14](#_Toc155179154)

[Appendix 3. ERM Criteria Model – Determining Likelihood and Impact 15](#_Toc155179155)

[Appendix 4. Summary table of UNDP Risk Management Roles and Responsibilities 17](#_Toc155179156)

[Appendix 5. Risk Committee Terms Of Reference 24](#_Toc155179157)

[Background 24](#_Toc155179158)

[Duties and Responsibilities 24](#_Toc155179159)

[Management Arrangement 25](#_Toc155179160)

[Appendix 6. Procedures 28](#_Toc155179161)

# Policy Scope and Objectives

Navigating through the complexity of multiple uncertainties is at the core of UNDP’s quest for innovative solutions to development and organizational challenges. UNDP’s Enterprise Risk Management (ERM) System is designed to allow the organization to be forward looking and manage the effect of uncertainties on objectives. The ultimate purpose of ERM is to **ensure foresight and risk-informed decisions** across all levels of the organization, thereby maximizing gains while avoiding unnecessary losses.

The scope of the ERM Policy covers risks across all levels of the organization, considering the internal and external context. **Risk** is defined asthe effect of uncertainty on organizational objectives, which could be either positive and/or negative (ISO 31000:2018; see [Appendix 1](#_Appendix_1._Terms) for all Terms and Definitions). This includes effects of UNDP activities on external factors, such as harm to people and the environment. UNDP ERM prioritizes preventing and managing potential negative effects but seeks to maximize positive effects where possible. UNDP ERM is concerned with:

* ***Institutional risk*.** Existing and emerging uncertainties that could facilitate or hinder the efficiency and effectiveness of core operations within the organization.
* ***Programmatic risk*.** Existing and emerging uncertainties that could facilitate or hinder the realization of programme or project objectives.
* ***Contextual risk*.** Existing and emerging uncertainties that could facilitate or hinder progress towards development priorities of a given society. ERM considers contextual risk when these external uncertainties also present institutional or programmatic risks.

ERM applies an integrated approachto risk management, with horizontal integration across all types of risks, and vertical integration from projects up to corporate level. By introducing an integrated and systematic approach to risk management the UNDP ERM Policy aims to:

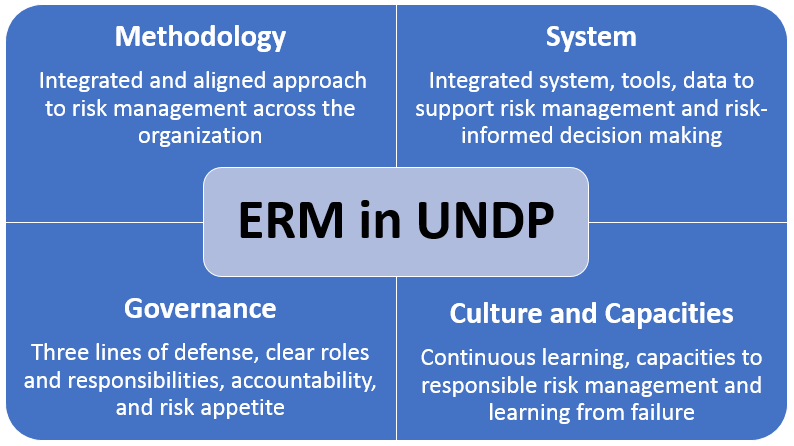
* Increase **programme effectiveness and relevance** through adaptive and informed decision-making
* Provide greater **assurance** regarding the management of significant risks
* Enable the exploration of **innovative solutions** to organizational and development challenges
* Inform effective and targeted allocation of **resources** to where they are most needed
* Enhance the **reputation** of UNDP as a value-driven and risk-informed organization
* Increase **efficiency** by safeguarding the accountable use of resources
* Safeguard **people and the environment**
* Manage and reduce to an acceptable level the **safety and security** risks to UNDPpersonnel, premises and assets.

While UNDP’s ERM Policy requires an integrated approach to risk management across the organization, risk management is a shared process with partners. In particular, risk needs to be viewed from a common UN system-wide perspective and considered at every step of the [UN Sustainable Development Cooperation Framework](https://unsdg.un.org/2030-agenda/cooperation-framework) (UNSDCF) process and through joint programming (refer to [UNSDCF Guidance](https://unsdg.un.org/resources/united-nations-sustainable-development-cooperation-framework-guidance)). Security risks are managed through the UN Security Management System.

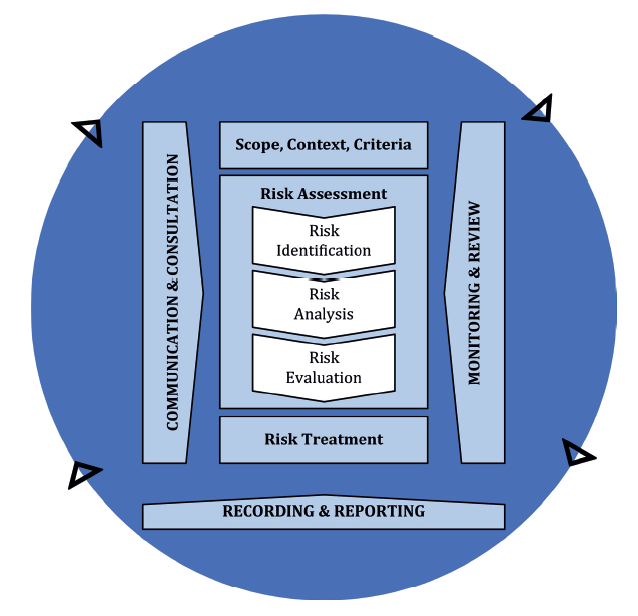
The ERM Policy is the umbrella framework for risk management in the organization. It brings together several prescriptive UN/UNDP policies and procedures which are applied to manage particular categories of risk when relevant, including:

* [Harmonized Approach to Cash Transfer](https://popp.undp.org/node/10891)
* [Capacity assessments (of partners and UNDP)](https://popp.undp.org/node/11531)
* [UNDP Anti-Fraud Policy](https://popp.undp.org/node/10426)
* UN Programme Criticality Framework
* [UNSMS Security Policy Manual – Policy on Security Risk Management](https://policy.un.org/policy-doc/30312)
* [Business Continuity Management](https://popp.undp.org/policy-page/business-continuity-management)
* [UNDP Policy on Due Diligence and Partnerships with the Private Sector](https://popp.undp.org/node/11301)
* [Programme/Project Quality Assurance](https://popp.undp.org/policy-page/quality-standards-programming)
* [Social and Environmental Standards and Screening Procedure](https://popp.undp.org/policy-page/social-and-environmental-standards)
* Theory of Change
* Audits and Evaluations
* [Procurement Ethics, Fraud and Corrupt Practices Policy](https://popp.undp.org/node/1506)
* [Procurement Strategy and Procurement](https://popp.undp.org/node/1426) Planning

To meet the policy objectives, UNDP’s ERM Policy is based on four pillars, summarized in the following diagram:



# ERM Methodology

The ERM methodology consists of six key elements in line with the ISO 31000:2018: communication and consultation; establishing scope, context, criteria; risk assessment; risk treatment; monitoring and review; and recording and reporting. These steps are applied across the whole organization:

1. at the project level (i.e. Development Projects, Engagement Facilities, Development Services, Institutional and Development Effectiveness Projects, Multi-Country and South-South Projects);
2. at the programme /unit level (i.e. Country Office/Programme, Regional Bureaux/Programme, Central Bureaux/Programme);
3. at the corporate level.

## 2.1 Risk Communication and Consultation

ERM requires an inclusive communication and consultation approach with all relevant stakeholders, including programmatic and operational staff as well as other relevant stakeholders (e.g. UN system, national partners, experts, donors, target groups and project affected people). Communication and consultation take place at regular/planned intervals to inform risk identification, assessment, treatment, monitoring, reporting and review.

## 2.2 Establishing the Scope, Context and Criteria

UNDP’s ERM Policy defines the scope and criteria for consistent risk management across the organization. Risk appetite may vary at the unit/office level based on the context and objectives.

Establishing the context requires understanding the external and internal context relevant for the realization of objectives at each level. **External context** includes but is not limited to social, cultural, environmental (including natural hazards and climate change), political, legal, financial, technological, security and economic factors. It also implies understanding the external stakeholders and their relationships, perceptions, and expectations. Similarly, **internal context** includes strategic objectives, values, standards, resources available, business processes, organizational culture, relationships with internal stakeholders, capacities, etc.

## 2.3 Risk Assessment

Risk assessment is the iterative process of risk identification, analysis, and evaluation. The objective is to provide sufficient information at appropriate intervals for risk-informed management decisions. High quality risk assessments enable greater acceptance of risk-taking opportunities (e.g. innovation) while ensuring rigorous due diligence, treatment, monitoring and control.

### Risk Identification

**Risk** is the effect of uncertainty on organizational and programming objectives, which could be either positive and/or negative. A risk, if realized, may enhance, prevent, degrade, accelerate or delay the achievement of objectives. Risk identification considers ‘future events’, their causes and potential impact. Therefore, risk identification requires understanding the context, historic risk patterns, and foresight thinking to reveal future scenarios and uncertainties relevant to the organizational goals and/or development results.

Potential risks across the ERM risk categories (see [Appendix 2](#_Appendix_2:_ERM)) should be considered to ensure that all relevant risks are identified.

Each identified risk, including those identified through relevant prescriptive processes listed above (e.g. HACT, SESP, Fraud risk assessment), is recorded in the Risk Register and is described in terms of cause, future event/scenario, and impact and assigned a category.

### Risk Analysis

Risk analysis requires an assessment of the **likelihood** of a risk and the potential **impact** on the objectives. The ERM Criteria Model (see [Appendix 3](#_Appendix_3:_ERM)) defines the five-point scale that is used to determine likelihood and impact. At the programme/unit and corporate level, a more detailed analysis of consequences is applied to determine overall impact. The capital support required to absorb unexpected losses is defined based on financial consequences.

Available information and evidence is considered in the assessment of likelihood and impact. Where applicable, the risk analysis includes the use of relevant thematic analyses (e.g. security risk analysis, fraud risk assessment, social and environmental impact assessment). In cases where likelihood and/or impact remain difficult to estimate and there is a potential for harm a precautionary approach is applied by estimating the worst-case scenario to ensure the risk is treated accordingly and closely monitored. The risk analysis should be adjusted if and when more information becomes available.

Based on the likelihood and impact the **risk significance** level (High, Substantial, Moderate or Low) is determined using the ERM Risk Matrix shown below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***UNDP ERM - Risk Matrix*** | | | | | | |
| **Impact** | ***5*** |  |  |  |  |  |
| ***4*** |  |  |  |  |  |
| ***3*** |  |  |  |  |  |
| ***2*** |  |  |  |  |  |
| ***1*** |  |  |  |  |  |
|  | ***1*** | ***2*** | ***3*** | ***4*** | ***5*** |
|  | **Likelihood**  *HIGH SUBSTANTIAL MODERATE LOW* | | | | | |

HIGH level risks require escalation and thorough risk analysis. Extra risk control mechanisms need to be put in place, and risk treatment measures clearly identified, budgeted, and implemented; frequent monitoring; and necessary precautions to ensure staff and personnel safety and security are not compromised and opportunities are not missed.

Both SUBSTANTIAL and MODERATE level risks require risk analysis scaled to the scope and nature of the risks with risk treatment and monitoring measures in place and budgeted. SUBSTANTIAL risks require more detailed risk analysis and risk management plans.

LOW level risks do not require further analysis or treatment.

### Risk Evaluation

Based on the analyses of individual risks, together with the defined risk appetite of the Unit/Office (aligned with the UNDP’s Risk Appetite Statement), an evaluation is made to determine which risks can be accepted and which risks require a priority response. Risks that present a potential for fraud or misuse of funds, significant harm to people or the environment and/or the organization should be avoided where possible and otherwise minimized and mitigated. Risk evaluation requires decision-making by line management at the relevant levels.

## 

## 2.4 Risk Treatment

### Risk Treatment Options

For each High, Substantial or Moderate level risk one or more risk treatment measures must be identified.

In case of threats to organizational objectives, risk treatment may be of four types: **terminate** (seeking to eliminate activity that triggers such a risk), **transfer** (passing ownership and/or liability to a third party), **mitigate** (reducing the likelihood and/or impact of the risk below the threshold of acceptability), and **tolerate** (tolerating the risk level).

In case of opportunities, risk treatment may be of four types: **exploit** (making the opportunity happen), **experiment** (testing new solutions in uncertain contexts), **enhance** (enhance the likelihood or impact through reinforcing the trigger condition or increasing exposure), and **accept** (no proactive actions).

### Risk Ownership and Escalation

All risks are assigned a **Risk Owner**, the individual who is ultimately accountable for ensuring the risk is managed appropriately. Each treatment measure is assigned a **Treatment Owner**, the individual who is responsible for executing the risk treatment. The Risk Owner and Treatment Owner may or may not be the same individual. Ownership is assigned based on the principle of who is ‘best suited’ to take accountability for managing the risk, noting that many people may need to be involved.

A risk is **escalated** when circumstances pertaining to the treatment itself may exceed the authority/mandate or expertise of the Risk Owner. If one or more of the following “escalation” conditions is met, the Risk Owner must escalate the risk:

* Risk treatment requires expenditures that are beyond what the Risk Owner is authorized to decide; and/or
* Risk cuts across, or may impact, multiple offices (e.g. reputational risk, changes to corporate policies); and/or
* Grievances from stakeholders have been received to which the Risk Owner cannot impartially and/or effectively respond (e.g. through UNDP’s Stakeholder Response Mechanism); and/or
* A serious security incident has occurred which has impacted UNDP personnel, facilities or programmes or the security environment has deteriorated requiring additional treatment measures and/or security advice; and/or
* When risk significance level is determined to be High.

When risks are escalated, the original Risk Owner must provide complete information to the receiving manager. The change of ownership takes place only after the receiving manager has confirmed that he/she accepts the ownership. A response to the request for risk transfer should be provided within 5 working days of receipt, in which period the risk ownership remains with the original Risk Owner. The escalation of the risk and the change of ownership must be noted in the Risk Register. If and when escalation is urgent, risk transfer should be completed within 24 hours and it is acceptable to communicate escalation using phone or e-mail and update the Risk Register afterwards.

Escalation follows the applicable line management, i.e. from project to programme to relevant Bureau (central/regional) and ultimately to the corporate level.

## 2.5 Risk Monitoring and Review

UNDP’s Risk Register provides an integrated platform for monitoring all levels and categories of risk. Regular **risk monitoring and review** is conducted to inform management decisions, enabling adaptive management and course corrections. The results of monitoring and review must be recorded and reported as appropriate and be used as a regular input to programme and project management decisions, audits, and organizational performance. While risk monitoring is customized to the specifics of each risk, the Risk Register needs to be updated if new information becomes available that effects the identification, analysis, evaluation and identified treatment measures. Real-time monitoring opportunities and threats should be considered in rapidly changing contexts to provide an early-warning mechanism and enable proactive response. In addition, the status and effectiveness of treatment measures needs to be monitored for Moderate, Substantial and High-level risks and included in programme and project management monitoring plans and budgets.

## 2.6 Recording and Reporting

**Risk reporting** ensures that relevant risk information is available across all levels of the organization in a timely manner to provide the necessary basis for risk-informed decision-making. Risk reporting must be carried out on a semi-annual basis at a minimum. A higher frequency of project risk monitoring and reporting might be necessary depending on the risk level and context (e.g. innovation projects or projects implemented in high security risk context, etc.). The following reports are required:

1. ***At the corporate level*** an annual report to the Executive Group (EG) and semi-annual reports to the Risk Committee (whereby the second semi-annual report is replaced by the annual report) are required. The Risk Committee submits the annual risk report to the EG based on a strategic analysis of the Integrated Work Plan (IWP) Risk Register.
2. ***At the programme/unit*** an annual report through the ROAR and semi-annual report through IWP Risk Register. The second semi-annual report is replaced by an annual report. The IWP Risk Register is informed by project-level Risk Registers and an analysis of cross-cutting programmatic, institutional and contextual risks. The IWP Risk Register is reviewed regularly by the Programme Manager to inform decision-making. Risk management must be reflected in mid-term and final evaluations. Programme Managers should also review and monitor projects’ risks and reflect and incorporate relevant risks in the IWP risk register.
3. ***At the project level*** theproject Risk Register is used for monitoring as often as needed, but no less than once a year. Reporting on project risk management is included in project progress reports (whatever the reporting cycle is) and reported to the Project Board. Risk management must also be evaluated and included in mid-term and final project evaluation reports.

In addition, **ad-hoc reporting** is often needed in crisis contexts or for High level risks that are time sensitive. The Risk Register is used to monitor these risks and inform ad-hoc reports. These reports must include an analysis of the risk, the initiated treatment/status and call for action or request for assistance.

Using its statutory power, UNDP maintains the right for **partial disclosure** of risks to the public to avoid any breach of its duty of confidentiality towards its beneficiaries or not to provoke any unwarranted losses of confidence towards its activities or its stakeholders.

# 3. ERM System

UNDP’s ERM system is designed to help UNDP staff and partners identify, analyze, monitor and report on existing and emerging risks. The **Risk Register** is a standard risk management tool to be used for all risk categories (e.g financial, programmatic, etc..) and at all levels within the organization. It is not only a monitoring and reporting tool but a management tool to strengthen risk management and inform decision making at all levels.

The **project Risk Register** reflects risks the project is facing. The **programme/unit Risk Register** reflects significant project-level risks determined to be relevant for the programme, cross-cutting programmatic risks, and those related to unit-level operations (HR, procurement, security, etc.). The **corporate Risk Register** reflects programme/unit-level risks determined to be critical for the organization and other risks that cut across the organization.

# 4. Governance

## 4.1 Three Lines of Defense

The “Three Lines of Defense”[[1]](#footnote-2) support more effective risk management by introducing structured governance and oversight that clarifies and segregates roles and responsibilities based on the following (see [Appendix 4](#_Appendix_4._Summary) for summary of risk management roles and responsibilities):

* First Line of Defense: functions that own and manage risks;
* Second Line of Defense: functions that oversee and or specialize in risk management, compliance;
* Third Line of Defense: functions that provide independent assurance.

### First Line of Defense

All UNDP personnel have a role in risk management and the first line of defense.

Accountability for ERM follows the line hierarchy, i.e., the line manager of each unit is accountable for risk management within his/her area of responsibility. This is identified in UNDP’s [Accountability Framework](https://popp.undp.org/node/3871).

* At the corporate level, the **Executive Group** is accountable for ERM and ensuring corporate decisions are risk-informed.
* At the programme/unit level:
  + The **Directors of Regional/Central Bureaux[[2]](#footnote-3)** are accountable for ERM and risk-informed decision-making at the Bureau level and are accountable to the Administrator. Bureau Directors ensure that the Programme Risk Registers for relevant Global/Regional Programmes are regularly updated, and identified risks are managed and escalated as needed. Directors of Bureaus also oversee the overall management of risks and controls within their bureaus and are responsible for ensuring that offices under their supervision keep their Risk Registers up to date, respond to risks appropriately, and report upwards in line as necessary.
  + For Country Offices/Programmes, the **Resident Representative (RR)/Head of Office** is ultimately responsible for ERM and accountable to the relevant Bureau Director for ensuring that the unit’s Risk Register is regularly monitored, updated, that risks are managed and that any risk that cannot be addressed at the unit level is escalated to the relevant Bureau.
  + For Country Offices/Programmes, the **Deputy** **Resident Representative** (or equivalent) assists the RR in managing risks related to achieving the objectives of the country programme, including programme delivery, quality, impact, reputation, and safeguards to people and the environment, and helps maintain an oversight role over functional areas within their area of responsibility.
  + Risk Focal Points have advanced knowledge of risk management challenges affecting their office/bureaus; and serve as the main point of contact between UNDP staff, Heads of Offices, the Regional/Central Bureau and the Risk Committee Secretariat.
* At the project level, the **Project Assurance** function (e.g., UNDP Programme Officer) is responsible for ensuring the Risk Register is regularly updated and monitored for the project and risk treatment measures are implemented.

### Second Line of Defense

The second line of defense is responsible for risk oversight, monitoring and technical support. This is a key function of UNDP’s **Risk Committee** (see [Appendix 5](#_Appendix_5._Risk) for the Risk Committee TOR)**,** a sub-committee of the Executive Group responsible for corporate risk reporting to the EG on a bi-annual basis, and when so requested. The Risk Committee is supported by the Risk Committee Secretariat. The Committee is chaired by the Associate Administrator, who is the Chief Risk Officer (CRO), with membership from UNDP senior management, invited experts and other relevant representatives may be invited to the Committee as needed. The main responsibilities of the Risk Committee are:

* Develop and propose the Risk Appetite Statement and Key Risk Indicators for UNDP;
* Ensuring that the overall risk framework is effective, relevant and applied corporately;
* Reviewing and analyzing the aggregated Risk Register and escalated risks on a regular basis with the purpose of identifying strategic risks and issues which require the attention of EG; and
* Developing proposals for managing escalated issues/risks (including Business Continuity Management and Incident & Crisis Management actions).

The Bureau for Management Services (BMS) and the Bureau for Policy and Programme Support (BPPS) are co-owners of the ERM policy and framework, and lead the revision and continuous improvement of ERM policy, guidance and tools to bring together programming and operations.

In addition, relevant technical experts (e.g. Security, Procurement, Financial, Operations, Legal, Programme and Project Management, Social and Environmental Standards), play an important role in the second line of defense, bringing technical oversight, knowledge, and support targeted to SUBSTANTIAL and HIGH-level risks.

The second line of defense also provides surge capacity to reinforce Country Offices facing high levels of risk. This includes responding to crisis, high risk contexts, potential or occurring harm to people and/or the environment, and opportunities for responsible risk-taking and innovation.

### Third Line of Defense

The third line of defense is the independent assurance and audit. UNDP’s Office of Audit and Investigations (OAI) play this role. It conducts audits to assess and provide assurance on the risk management framework and practices in the organization and provide recommendations on ways to improve risk management.

# 5. Risk Management Culture

UNDP recognizes that mindsets and behaviors of individuals and groups inside the organization play a crucial role in the effective execution of ERM. A mature risk management culture is characterized by the following:

* Risk-informed decision making at all levels, including flexibility for adaptive management and course correction.
* Responsible risk-taking and innovation is rewarded.
* ‘Failures’ are acknowledged and recognized as part of the learning curve, particularly while operating in complex contexts.
* Continuous learning for strengthened risk management capacities.
* Key stakeholders are involved in all stages of the risk management process.
* Absence of approaching risk management purely as a compliance issue.
* Open communication on all risk management issues and lessons learned and a culture of “working out loud.”
* Effective risk escalation when needed.
* Adequate resource allocations for risk management at all levels.
* UNDP personnel are enabled to ‘stay and deliver’ at an acceptable level of security risk.

# Appendix 1. Terms and Definitions

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

**Consequence.** Is the effect that may result from a risk being materialized. There might be several consequences of a risk, including cascading effects.Often, the total impact of a risk is broader than the sum of all its consequences.

**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.

**Impact.** The totality of all effects of an event affecting objectives.

**Likelihood.** The chance of something happening.

**Risk.** The effect of uncertainty on organizational objectives, which could be either positive and / or negative (ISO 31000:2018). Risk is described as a ‘future event’, with its causes and its potential consequences. UNDP ERM is concerned with:

* ***Institutional risk*.** Existing and emerging uncertainties that could facilitate or hinder the efficiency and effectiveness of core operations within the organization.
* ***Programmatic risk*.** Existing and emerging uncertainties that could facilitate or hinder the realization of programme or project objectives.
* ***Contextual risk*.** Existing and emerging uncertainties that could facilitate or hinder progress towards development priorities of a given society. ERM considers contextual risk when these external uncertainties also present institutional or programmatic risks. Note that some contextual risks may fall under established risk management practice and definitions that need to be considered (e.g. for climate and disaster risk).

**Risk appetite.** The amount and type of risks that projects, programmes/units, and UNDP as a whole is willing to take in order to meet its strategic objectives at each level respectively.

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

**Risk categories.** A risk classification system in relation to what organization does to help to systematically identify and track the risks across its main areas of performance.

**Risk escalation:** Transfer of risk ownership to the next in line in the organizational hierarchy.

**Risk level.** Significance of a risk, expressed as the combination of impact and likelihood.

**Risk management.** Coordinated activities to direct and control an organization with regard to risk at all levels. Risk management is concerned with exploring new opportunities and avoiding negative consequences within the realization of UNDP Strategy.

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

**Risk owner.** The individual who is accountable for ensuring a risk is managed appropriately.

**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, a programme or project, or as otherwise defined.

**Risk Register.** A risk management tool that serves as a record of all risks across the organization, including at the project level, programme/unit level, and corporate level. For each risk identified, it includes the following information: risk ID, risk description (cause, event, consequences), likelihood, impact, significance level, risk category, risk owner, risk treatment action, risk escalation, and risk status.

**Risk treatment.** A measure to modify risk exposure to provide reasonable assurance towards the achievement of objectives. This includes risk treatment, which is response to negative events, and opportunity management, which is response to positive events.

**Treatment owner**. The individual who is responsible for executing the risk treatment.

# Appendix 2. ERM Risk Categories and Sub-Categories

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1.Social and Environmental** | **2. Financial** | **3.Operational** | **4.Organizational** | **5. Reputational** | **6. Regulatory** | **7. Strategic** | **8. Safety and Security** |
| * 1. Human rights   2. Gender equality and women’s empowerment   3. Grievances (Accountability to stakeholders)   4. Biodiversity conservation and sustainable natural resource management   5. Climate change and disaster risks   6. Community health, safety and security   7. Cultural heritage   8. Displacement and resettlement   9. Indigenous peoples   10. Labour and working conditions   11. Pollution prevention and resource efficiency   12. Stakeholder engagement   13. Sexual exploitation and abuse | * 1. Cost recovery   2. Value for money   3. Corruption and fraud   4. Fluctuation in credit rate, market, currency   5. Delivery   6. Budget availability and cash flow | * 1. Responsiveness to audit and evaluations (Delays in the conduct of and implementation of recommendations)   2. Leadership and management   3. Flexibility and opportunity management   4. Reporting and communication   5. Partners’ engagement   6. Transition and exit strategy   7. Occupational safety, health and well-being   8. Capacities of the partners | * 1. Governance   2. Execution capacity   3. Implementation arrangements   4. Accountability   5. Monitoring and oversight   6. Knowledge management   7. Human Resources   8. Internal control   9. Procurement | 5.1. Public opinion and media  5.2. Engagement with private sector partnership  5.3. Code of conduct and ethics  5.4. Communications  5.5. Stakeholder management  5.6. Exposure to entities involved in money laundering and terrorism financing | * 1. Changes in the regulatory framework within the country of operation   2. Changes in the international regulatory framework affecting the whole organization   3. Deviation from UNDP internal rules and regulations | * 1. Alignment with UNDP strategic priorities   2. UN system coordination and reform   3. Stakeholder relations and partnerships   4. Competition   5. Government commitment   6. Change/turnover in government   7. Alignment with national priorities   8. Innovating, piloting, experimenting | 8.1. Armed conflict  8.2. Political instability  8.3. Terrorism  8.4. Crime  8.5. Civil unrest  8.6. Natural hazards  8.7. Manmade hazards  8.8. Cyber security and threats |

NOTE: ERM Risk categories that relate to the Quality Standards for Programming will be mapped accordingly and reflected in Risk Register/QA system.

# Appendix 3. ERM Criteria Model – Determining Likelihood and Impact

**Determining Likelihood (at Project, Programme/Unit, Corporate levels):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood | Not likely | Low likelihood | Moderately likely | Highly likely | Expected |
| **1** | **2** | **3** | **4** | **5** |
| Description  (“The risk is expected to materialize….”) | Every 5 years or less  **and/or**  very low chance (<20%) of materializing | Every 3-5 years  **and/or**  low chance (20% - 40%) of materializing | Every 1-3 years  **and/or**  chance of materializing between 40% - 60% | Once or twice a year  **and/or**  high chance of materializing (60% - 80%) | Several times a year  **and/or**  chance of materializing above 80% |

**Determining Impact:**

***Project Level –***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact | Negligible | Minor | Intermediate | Extensive | Extreme |
| **1** | **2** | **3** | **4** | **5** |
| Description  (“If the risk materializes,….”) | Negligible/no impact on project results, positive or negative. Negligible or no potential adverse impacts on people and/or environment. | 5-20 % of the applicable and planned results affected, positively or negatively. Potential adverse impacts on people and/or environment very limited and easily managed. | 20-30% of the applicable and planned results affected positively or negatively. Potential adverse impacts on people and/or environment of low magnitude, limited in scale and duration, can be avoided, managed or mitigated with accepted measures. | 30-50% of the applicable and planned results/outcome affected positively or negatively. Potential adverse impacts on people and/or environment of medium to large magnitude, spatial extent and duration. | More than 5O% of the applicable and planned results/outcome affected positively or negatively. Adverse impacts on people and/or environment of high magnitude, spatial extent and/or duration. |

***Programme/Unit and Corporate Levels –***

The following analyses of potential consequences for the organization are conducted for each risk. **Overall risk IMPACT is then determined based on the highest level of impact.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Impact | | Negligible | Minor | Intermediate | Extensive | Extreme |
| **1** | **2** | **3** | **4** | **5** |
| Description of consequence | **Financial**  **(absolute and relative)** | Estimated range in USD, 3 numbers:   * Maximum (highest level of potential deviation, +/-)) * Likely (*best guess*) * Minimum (*lowest level of potential deviation, +/-)* )   which, based on best guess figure, corresponds to: | | | | |
| <5 % deviation from applicable budget | 5-20 % deviation from applicable budget | 20-30% deviation from applicable budget | 30-50% deviation from applicable budget | >50% deviation from applicable budget |
| **Development results** | Negligible/no impact on results/outcome, positive or negative | 5-20 % of the applicable and planned results/outcome affected, positively or negatively | 20-30% of the applicable and planned results/outcome affected, positively or negatively | 30-50% of the applicable and planned results/outcome affected, positively or negatively | More than 5O% of the applicable and planned results/outcome affected, positively or negatively |
| **Operations** | Delay or acceleration of applicable operations by 1-2 days | Delay or acceleration of applicable operations 2-7 days | Delay or acceleration of applicable operations 1-4 weeks | Delay or acceleration of applicable operations for one month or longer | Permanent shift in applicable operations |
| **Compliance** | Negligible deviation from applicable rules and regulations | Moderate deviation from applicable rules and regulations | Deviation from applicable rules and regulations | Significant deviation from applicable rules and regulations | Major deviation from applicable rules and regulations |
| **Safety & Security** | No Effect on UNDP Personnel,  and/or  No effect on UNDP Operations and programmes | Slightly Injurious Effect on UNDP Personnel  and/or  injuries to general population directly or indirectly caused by UNDP actions | Moderately Injurious or Psychologically Traumatic Effect and/or  major injuries to general population directly or indirectly caused by UNDP actions | Fatal (individual or small numbers), Severely Injurious or Severely Psychologically Traumatic Effect  and/or  loss of life to general population directly or indirectly caused by UNDP actions | Catastrophically Fatal Effect (mass casualties)  and/or  loss of life to general population directly or indirectly caused by UNDP actions |
| **Reputation** | Isolated negative or positive comments from external stakeholders | Several negative or positive comments from external stakeholders | Negative or positive reports/articles in national, regional  and/or international media | Negative or positive 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 or positive 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 4. Summary table of UNDP Risk Management Roles and Responsibilities

| **Title** | **Role** | **Responsibilities** |
| --- | --- | --- |
| ***First line of defense*** | | |
| **All UNDP Personnel** (at country, regional and headquarters levels)  *(Project, programme/Unit, and Corporate Levels)* | All UNDP personnel have a role in risk management and the first line of defense. Personnel are responsible for identifying and managing the risks that affect the achievement of objectives related to their areas of work within their delegated authority.  Personnel must communicate regularly to their supervisors any risk that they cannot effectively respond to or those that are beyond their authority to mitigate. They are accountable for ensuring compliance with various control activities and ensuring that these are adequately evidenced. | * Support the identification and management of risks in their Business Unit or Country Office. * Escalate risk management issues and concerns beyond their authority to the Head of Office as appropriate. |
| **Executive Group**  *(Corporate Level)* | The Executive Group is accountable for ERM implementation. | * Ensuring corporate decisions are risk-informed and incompliance with UNDP policies and regulations. |
| **Regional and Central Bureau Directors[[3]](#footnote-4)**  *(Programme/Unit Level)* | Bureau Directors as head of bureaus oversee the overall management of risks and controls within their bureaus, including COs/BUs. | * Maintain effective implementation of risk management framework within their bureau and assign risk owners at the bureau level. * Provide effective leadership in risk management and ensure that suitable staff are assigned accountability for managing risk within their areas of responsibilities and authority. * Monitor risks and risk treatments and ensure that risks are within the appropriate risk appetite levels. * Chair bureau risk discussions to review risk information including indicators and appetite metrics and follow-up on mitigation measures. * Lead the efforts to ensure that internal and external oversight and compliance recommendations are effectively addressed, as relevant. * Provide consultative, technical and resource assistance to escalated risk from offices. * Approve or reject risks which are escalated to the bureau. * Escalate risks to the Risk Committee as appropriate. |
| **Head of Offices (HoO) for Central Bureaus**  *(Programme/Unit Level)* | As Head of Offices, identify and manage risk impacting their office’s Integrated Work Plans (IWPs) and maintain an oversight role over functional areas within their areas of responsibility. | * Leads and approves regular identification of risks and proactively manages and mitigates them as per the UNDP risk management framework for delivery of the office’s IWP results, ensuring availability of funds and expertise to mitigate risks, as required. * Maintains strategic oversight of IWP Risks, and any other risks of high severity emanating from the IWP annual risk assessment. * Escalates any risks that require attention of the respective bureau or the corporate Risk Committee as per the ERM policy. |
| **Resident Representatives (RRs)**  *(Programme/Unit Level)* | As Head of Country Offices, manages risks related to achieving the objectives of the country programme, including programme delivery, quality, impact, reputation, and safeguards to people and the environment, and maintain an oversight role over functional areas within their countries of responsibility. | * Maintains strategic oversight of Country Programme Risks, high-risk projects and portfolios and any other risks of high severity emanating from risk assessment tools. * Leads and facilitates regular identification of country programme risks. * Proactively identifies, manages and mitigates risks as per UNDP risk management framework for delivery of country programme results, ensuring availability of funds and expertise to mitigate risks, as required. * Escalates any risks that require attention of the bureau or the corporate risk committee as per the ERM policy. * Chairs the local project appraisal committee to review the proposed project’s quality and the capacity of the implementing partner to deliver, including the risk mitigation measures/strategy. |
| **Deputy Resident Representatives (DRRs) or equivalent**  *(Programme/Unit Level)* | Assists the RR in managing risks related to achieving the objectives of the country programme, including programme delivery, quality, impact, reputation, and safeguards to people and the environment, and helps maintain an oversight role over functional areas within their area of responsibility. | * Assists the RR in identification, mitigation planning and as required, escalating country-level risks, and the implementation of the risk management framework in order to deliver country programme results and achieve impact.  She/he works closely with the CO team to ensure risks treatments are up to date, implemented and on track. * Supports the RR in maintaining oversight of high-risk projects and portfolios, and risks of high severity emanating from projects and the various risks assessment tools, to ensure necessary and timely follow up action. * Review the proposed project’s quality and the capacity of the implementing partner to deliver, including the risk mitigation measures/strategy. |
| **Risk Focal Points**  (Risk Specialist/advisors, M&E Officer, Head of PMSU, Operations Manager, Programme Officer, etc.)  *(Programme/Unit Level)* | Risk Focal Points (FPs) or risk specialist/advisors are designated for risk management issues in UNDP Bureaus or offices at country, regional and headquarters levels.  Risk Focal Points are Heads of Operations, Monitoring and Evaluation Officers, Risk advisors or others appointed by the Heads of Office (HoOs); they have advanced knowledge of risk management challenges affecting their office/bureaus; and serve as the main point of contact between UNDP staff, Heads of Offices, the Regional/Central Bureau and the Risk Committee Secretariat. | * Champion risk management practices in the office/bureau and train staff on UNDP’s ERM framework and risk management processes. * Collect and analyze risk information for sharing with the Head of Office (HoO) and support the escalation of risks by HoO/Risk Managers to Bureaus and/or the Risk Committee Secretariat based on the escalation criteria in the ERM policy. * Ensure that risks are reviewed and updated in the risk registers in Quantum and Quantum+. * Support bureau/region/country senior management in overseeing the effectiveness of risk management practices by, for example, identifying potential risk treatments to reduce risk levels, monitoring of risk treatments, etc. * Participates in project appraisal to provide inputs including formulating risk management plans during project designs. * Ensures relevant colleagues and stakeholders from both programme and operations are consulted in the identification and management of risks for all projects and portfolios in the office/unit, and for the programme, if applicable. |
| **Project Assurance** (at country, regional and headquarters levels)  *(Project Level)* | The Project Assurance function (e.g., UNDP Programme Officer) has a role in risk management and the first line of defense. | * Ensure the Risk Register is regularly updated and monitored for the project and risk treatment measures are implemented. |
| ***Second line of defense*** | | |
| **Risk Committee** | The Risk Committee is a sub- committee of the Executive Group (EG) that oversees the overall implementation, and use, of UNDP’s Enterprise Risk Management framework across UNDP and advises on the management of corporate risks facing UNDP at the highest level. | * The Committee is chaired by the Associate Administrator. * Oversight of UNDP risk management policies and practices framework. * Focus on strategic corporate risks that are escalated to the committee. * Responsible for identifying corporate risks, deciding how they will be managed and treated, and reporting to the EG. * Assist the Executive Group in fulfilling its responsibilities regarding identifying and assessing the strategic risks facing UNDP, and its oversight responsibilities regarding UNDP’s risk appetite, the organization’s performance in managing risk, the risk management framework and the governance structure that support it. * Recommend, for the EG’s approval, the ERM framework and appropriate resources to maintain UNDP’s risk management framework. |
| **Risk Committee Secretariat** | The Risk Committee Secretariat assists the Risk Committee Chair and Committee members in effective and efficient management of committee meetings. | * Prepare agenda and background materials for Risk Committee meetings. * Ensure proper documentation of Risk Committee decisions. * Conduct the analysis of aggregated risk logs as part of corporate risk analysis. * Record and present escalated risks for Risk Committee deliberations. * Perform any other tasks as assigned by the chair of the Committee. |
| **Chief Risk Officer**  (Associate  Administrator) | The Associate Administrator is the ultimate champion of ERM at UNDP. | * Provide leadership to ensure UNDP’s Risk Management Framework (i.e., policy, approaches and tools) is effective and fit for purpose and oversee its implementation across UNDP. * Promote a culture of risk management that is pro-active, agile and anticipatory. * Serve as the Chair of the Risk Committee and promote an optimum accountability system for the organization. * Ensure effective identification, analysis, treatment and monitoring of corporate risks facing the organization by the risk owners and approve the corporate risk register in consultation with the Risk Committee members. * In collaboration with bureau leaders, promote strengthened links between project and portfolio level risks, programme/unit level risks and corporate level risks, with the view of ensuring systemic/holistic risk management and mitigation. Provide recommendations to respective bureau(s) on escalated high-risk partnerships, as relevant. * Serve as the Senior Designated Officer (SDO) for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy implementation at UNDP. |
| **BMS/BPPS**  **(ASG)** | Co-owners of the ERM policy and framework, responsible for leading the revision and continuous improvement of ERM policy, guidance and tools to bring together programming and operations. | * Develop and update UNDP’s Risk Management Framework and lead the continuous improvement of corporate risk management approaches, processes and tools. * Promote a culture of responsible risk management and contribute to embedding the principles and requirements for effective risk management in the roles and responsibilities of all staff, including through training and knowledge sharing. * Ensure risk management frameworks, policies and procedures and systems are fit for purpose and executed effectively, including processes for managing risk exposures. * Maintain, update and communicate the policy and related procedures and guidance to ensure alignment with UNDP’s evolving risk management framework and risk appetite. * Ensure risk management practices are integrated into strategic planning, programmes, operations, monitoring and evaluation processes. * Lead the effort of designing and implementing relevant corporate risk management policies and procedures. |
| **Relevant Technical Experts** (e.g., Chief of Finance, Operations, Legal, ITM, Human Resources, Security, Procurement, Partnership, Programme and Project Management, Social and Environmental Standards, etc.) | Establishes comprehensive risk-control framework for the functional area/business process for which they have been designated as process/risk owners. | * Help in the identification and mitigation of risks related to their functional area in collaboration with relevant risk owner(s), and provide input into the update of relevant risk registers, as applicable. * Put in place adequate second-line controls to ensure that internal control operate effectively and mitigate the risks identified and report on their results. |
| ***Third line of defense*** | | |
| **Office of Audit and Investigations (OAI)** | OAI provides independent assurance and audit. | * Conduct audits to assess and provide assurance on the risk management framework and practices in the organization and provide recommendations on ways to improve risk management. |

# Appendix 5. Risk Committee Terms Of Reference

### 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 ERM Policy 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 bi-annual 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).

1. 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.

1. Analysis from aggregated Risk Register;

On a bi-annual 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.

1. Escalated risks from bureau and units

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.

1. ***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), Incident and Crisis Management (ICM), and Risk Reserves.

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 applied 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 relevant policies are proposed to the Executive Group (EG) for endorsement.

The Risk Committee also reviews and recommends the Risk Appetite Statement for UNDP, to the EG for approval. The statement should be reviewed and updated as needed.

1. ***Corporate Vetting Committee (CVC)***

UNDP’s Risk Committee also serves as the Corporate Vetting Committee. Experts and other relevant representatives may be invited, as required, to support the committee’s deliberations. The CVC is responsible for providing advice to the Senior Designated Officer (SDO)[[4]](#footnote-5) on the following:

1. Decision-making with regards to AML/CFT matters, including:

* Business relationships with high-risk counterparties;
* Counterparty relationships to be exited, prohibited and/or added to the “[Internal Excluded List](https://popp.undp.org/node/4066)”;
* Counterparties to be added to the “[Dispensation List](https://popp.undp.org/node/4066)”; and
* Any other related matters that require consideration and decision-making at the senior level as deemed fit by the SDO.

1. Implementation and refinement (as required) of the AML/CFT policy, processes, tools and pilot programs.

### 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 bi-annual 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;
* Directors of all Regional Bureau
* Director of the Bureau for Management Services;
* Director of BERA
* Director of BPPS
* Director of CRU;
* Chief Finance Officer;
* Director of Security Office;

The membership to the 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;
* Vertical fund managers;
* Deputy Bureau Directors;
* Expert or resource persons on particular issues;
* Other staff as necessary.

1. ***Relationship with Other Corporate Decision-Making Structures***

The Risk Committee is a sub-committee to the Executive Group. It provides reports to the EG bi-annually and/or as needed. The relationship with other corporate decision-making structures can be depicted as follows:

The Risk Committee reviews, analyses and makes decisions about risks that are identified through the different corporate mechanisms and data sources (e.g. OPG, ET, SMG, Crisis Board, Risk Register). 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 periodic Risk Committee meetings.

1. ***Risk Committee Meetings***

The Risk Committee shall meet bi-annually, preferably during the week when the EG meeting is scheduled but before the EG meeting takes place. On and ad-hoc basis, the chair of the Risk Committee can also call for a Committee meeting for immediate deliberation of any urgent risk issues. The standing agenda for the Committee meeting is as follows:

* Review the effectiveness of the ERM implementation (including the policies, procedures, learning and other tools);
* Review of the Executive Team decisions and mechanisms;
* Review and manage corporate risks, including analysis of emerging trends and risks impacting the organization (including review of aggregated corporate Risk Register and KRIs);
* Review Risks of Level 3 Crisis Countries - led by Regional Bureaux
* Any other business

1. ***Risk Committee Secretariat***

The Risk Committee is supported by a secretariat (Risk Management Specialists) 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.

# Appendix 6. Procedures

Procedures for Managing **Project-Level Risk** (Country, Regional or Global Projects)

| **Steps** | **Responsible Party** | **Template/Guidelines** | **Explanatory Note** |
| --- | --- | --- | --- |
| **1- Communications & Consultation** | Risk Owner |  | Engage key stakeholders in risk identification and risk analysis process. Keep the Project Board and other stakeholders/partners informed on RM processes at the project level. |
| **2- Scope, context and Criteria** | Project Developer or  Project Manager | [Project Document Template](https://popp.undp.org/node/1131)  [Project Risk Register](https://popp.undp.org/node/326) | Integrated in Programme and/or Project Document, Multi-Year Work Plan |
| **3- Risk Assessment:**  Identification of Risks | Project Developer or  Project Manager | [Project Risk Register](https://popp.undp.org/node/326) | Assess risks during Project Design and as often as needed during implementation, once a year at a minimum. Track in Risk Register.  In consultation with relevant stakeholders, identify major risks for the project objectives. |
| Risk Analysis | Project Developer or  Project Manager | [Project Risk Register](https://popp.undp.org/node/326) | Analyze likelihood and impact of the project risks by applying the ERM Criteria Model and record in Risk Register. |
| Evaluation of Risk | Project Manager | [Project Risk Register](https://popp.undp.org/node/326) | Evaluate each project risk to determine which risks can be accepted and which risks require a priority treatment in order to meet project objectives and avoid harm. |
| **4- Risk Treatment** | Project Developer or  Project Manager | [Project Risk Register](https://popp.undp.org/node/326)  [Risk Escalation Guideline](https://popp.undp.org/node/4001) | Identify risk treatment measures in Risk Register during project design, prior to project approval.  During implementation, update/confirm risk treatment measures to address changes in context, new information and new risks, as necessary and based on Step 4. Implement identified risk treatment measures. Escalate/transfer the risks that meet any of the escalation conditions to the applicable line management. |
| **5 - Risk Monitoring & Review** | Risk Owner | [Project Risk Register](https://popp.undp.org/node/326) | Monitor and review risks at the frequency that is best fit for the risk and complexity of the project. Update Risk Register once a year at a minimum. |
|  |
| **6-Risk Recording and Reporting** | Project Manager | [Project Risk Register](https://popp.undp.org/node/326) | Risks are to be recorded in ERM Risk Register and risk reporting is integrated in agreed project reporting cycle, once a year at a minimum. Project risks presented to the Project Board. |

Procedures for Managing **Unit/Programme**-Level Risk

|  |
| --- |
| **COUNTRY OFFICE/PROGRAMME** |

| Steps | Responsible Party | Template/Guidelines | Explanatory Note |
| --- | --- | --- | --- |
| **1- Communications & Consultation** | Risk Owner |  | Engage key stakeholders in risk identification and risk analysis process. Keep the Programme Board, other stakeholders/partners of the CO and the HQ Unit informed on RM processes. |
| **2 - Scope, context and Criteria** | Programme Manager /Resident Representative | [UNSDCF Guidance](https://unsdg.un.org/resources/united-nations-sustainable-development-cooperation-framework-guidance)  [CPD Template](https://popp.undp.org/node/1816)  [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Integrated in the [UN Sustainable Development Cooperation Framework](https://unsdg.un.org/2030-agenda/cooperation-framework) (UNSDCF); Country Programme Document (CPD); IWP of the CO and the HQ Unit |
| **3 – Risk Assessment**  Identification of Risks | Programme Manager in consultation with relevant expertise | [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | In consultation with relevant stakeholders, identify major risks for the overall programme objectives and the respective IWP of the CO and the Unit and track in programme/unit Risk Register, during project design and twice a year at a minimum during implementation. |
| Risk Analysis | Programme Manager in consultation with relevant expertise | [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Analyze likelihood and impact of programme/unit risks by applying the ERM Criteria Model and record in Risk Register. |
| Evaluation of Risk | Programme Manager in consultation with relevant expertise | [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Evaluate each risk in the Programme Risk Register specific to Country Offices to determine which risks need treatment and must be prioritised, in order to meet the objectives of the respective IWP. |
| **4- Risk Treatment** | Programme Manager in consultation with relevant expertise | [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home)  [Risk Escalation Guideline](https://popp.undp.org/node/4001) | Implement treatment options. Respond to the escalated risks. Escalate the risks that can't be adequately addressed at the CO and HQ Units to Programme level. |
| **5 - Risk Monitoring & Review** | Risk Owner | [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Monitor risks at the frequency that is best fit for the risk and complexity of the Programme/Unit. Update Risk Register on bi-annual basis at a minimum. |
|  |
| **6 Risk Recording and Reporting** | Programme Manager in consultation with relevant expertise | [Programme/Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Record risks in ERM risk Register and Report the CO and HQ Units major risks in their IWP bi-annually and annually in ROAR. |
| **REGIONAL/CENTRAL BUREAUX/PROGRAMMES** | | | |
| Steps | Responsible Party | Template/Guidelines | Explanatory Note |
| **1- Communications & Consultation** | Risk Owner |  | Include key stakeholders in risk identification and risk analysis process. Communicate & consult with relevant parties of the Bureau and the Office at all stages of RM processes and update them at regular/planned intervals. |
| **2- Scope, context and Criteria** | Bureau Director/Designate | [Project Document Template](https://popp.undp.org/node/1131)  [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home)  [Examples of financial quantification of identified risk](https://popp.undp.org/node/3886) | Integrated in Regional Programme Document; Global Programme Document; Bureau IWP; Office IWP |
| **3- Risk Assessment**  Identification of Risks | Bureau Director/ Designate | [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | In consultation with relevant stakeholders, identify major risks for the overall objectives across COs in the region, Central Bureaux or the Office level, and track in respective IWPs (Risk Register), during programme design and twice a year at a minimum during implementation. |
| Risk Analysis | Bureau Director/ Designate | [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Analyze likelihood and impact of programme/unit risks by applying the ERM Criteria Model and record in Risk Register. |
| Evaluation of Risk | Bureau Director/ Designate | [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Evaluate each risk in the Programme/Unit Risk Register specific to Regional/Central Bureaus to define which risks require priority treatment based on the Bureau & Office’s risk acceptance in order to meet the Programme objectives and avoid harm. |
| **4- Risk Treatment** | Bureau Director /Designate | [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home)  [Risk Escalation Guideline](https://popp.undp.org/node/4001) | Respond to the COs & Units' escalated risks; Escalate the risks that cannot be adequately addressed by Central/Regional Bureaux, and the Offices to the Risk Committee. |
| **5- Risk Monitoring & Review** | Risk Owner | [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Monitor risks at the frequency that is best fit for the risk and complexity of the Programme/Unit. Update Risk Register on bi-annual basis at a minimum. For RBx, ensure risk management being conducted in COs across the region. |
|  |
| **6 Risk Recording and Reporting** | Bureau Director/ Designate | [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Records Risks in the ERM risk register and Report the Bureau and the Offices' major risks bi-annually in IWP and annually in ROAR. |

Procedures for Managing **Corporate Risk**

| **Steps** | **Responsible Party** | **Template/Guidelines** | **Explanatory Note** |
| --- | --- | --- | --- |
| **1- Communications & Consultation** | Risk Owner |  | Include key stakeholders in risk identification and risk analysis process. Communicate UNDP risk profile to EG through annual reporting cycle. |
| **2- Scope, context and Criteria** | Risk Committee | [Risk Committee TORs](https://popp.undp.org/node/18926)  [Examples of financial quantification of identified risk](https://popp.undp.org/node/3886) | Integrated in UNDP Strategic Plan (SP) |
| **3 - Risk Assessment**  Identification of Risks | Risk Committee | [Corporate Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Identify major risks (both threats & opportunities) at corporate level affecting UNDP, twice a year at a minimum. |
| Risk Analysis | Risk Committee | [Corporate Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Review and analyze the overall UNDP risk profile and present to Risk Committee. |
| Evaluation of Risk | Risk Committee | [Corporate Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Evaluate each risk in the Corporate Risk Register to define the risks that require priority treatment based on UNDP’s risk acceptance in order to meet its objectives in the Strategic Plan and avoid harm. |
| **4- Risk Treatment** | Risk Committee | [Corporate Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Escalate the risks from HQ units & all Bureaux for Risk Committee consideration to make decisions on escalated corporate risks (prioritize them and specific actions to be taken). |
| **5 - Risk, Monitoring & Review** | Risk Owner | [Corporate Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Document the decisions taken by Risk Committee in the Corporate Risk Register, and monitor and update it regularly. |
|  |
| **6 Risk Recording and Reporting** | Risk Committee | [Corporate Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | Records Risks in the ERM risk Register and Report the overall risk profile of UNDP; Prepare a bi-annual report to the EG, based on a strategic analysis of UNDP's overall risk landscape. |

1. *The Three Lines of Defense in Effective Risk Management and Control*, (Altamonte Springs, FL: The Institute of Internal Auditors Inc, January 2013) is embedded in the UN Risk Management, Oversight and Accountability Model. [↑](#footnote-ref-2)
2. In addition, the UNV Executive Coordinator and UNOSSC Director for UNV and UNOSSC respectively. [↑](#footnote-ref-3)
3. In addition, the UNV Executive Coordinator and UNOSSC Director for UNV and UNOSSC respectively. [↑](#footnote-ref-4)
4. The Senior Designated Officer (SDO) is responsible for ensuring the effective implementation of the AML/CFT policy at UNDP and decision-making on matters presenting heightened risks to the organization, including escalated cases. The role of the SDO is assigned to the Associate Administrator (AA). The AA also serves as UNDP's Chief Risk Officer. [↑](#footnote-ref-5)