

**UNDP Enterprise Risk Management (ERM)**

**Policy and Procedures**

**Policy Owner: BMS/BPPS**

Contents

[1. Policy Scope and Objectives 3](#_Toc210748792)

[2. ERM Methodology 5](#_Toc210748793)

[3. Risk Ownership and Escalation Criteria 8](#_Toc210748794)

[4. ERM System 9](#_Toc210748795)

[5. Governance 9](#_Toc210748796)

[5.1 Three Lines Model 9](#_Toc210748797)

[5.2 Key Roles and Responsibilities 11](#_Toc210748798)

[5.2.1 First Line Roles 12](#_Toc210748799)

[5.2.2 Second Line Roles 13](#_Toc210748800)

[5.2.3 Third Line Role 14](#_Toc210748801)

[6. Risk Management Culture 14](#_Toc210748802)

[Appendix 1. Terms and Definitions 15](#_Toc210748803)

[Appendix 2. ERM Risk Categories and Sub-Categories 17](#_Toc210748804)

[Appendix 3. ERM Criteria Model – Determining Likelihood and Impact 18](#_Toc210748805)

[Appendix 4. Summary table of UNDP Risk Management Roles and Responsibilities 20](#_Toc210748806)

[Appendix 5. Risk Committee Terms of Reference 29](#_Toc210748807)

[Background 29](#_Toc210748808)

[Duties and Responsibilities 29](#_Toc210748809)

[Management Arrangement 31](#_Toc210748810)

[Appendix 6. Procedures 34](#_Toc210748811)

# 

# Policy Scope and Objectives

1. 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) policy 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.
2. 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[[1]](#footnote-2); 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, portfolio, 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.

1. ERM applies an integrated approachto risk management, with horizontal integration across all types of risks, and vertical integration from projects and/or portfolios up to the programme/unit, bureau and corporate levels. By introducing an integrated and systematic approach to risk management, the UNDP ERM Policy aims to:

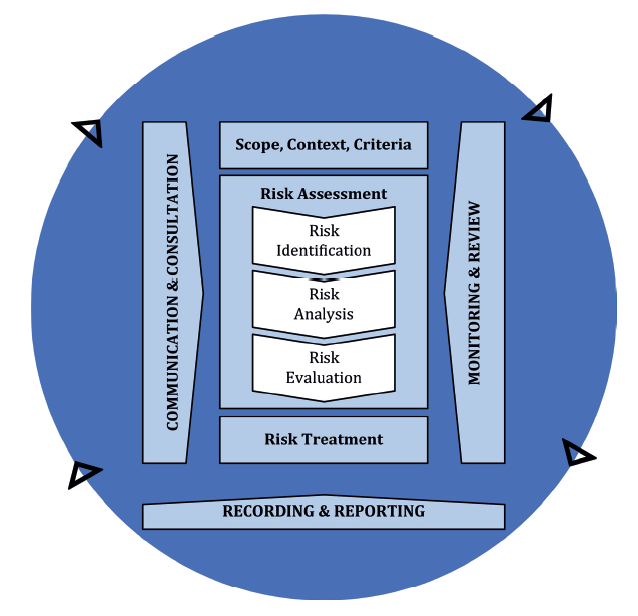
* Increase **programme effectiveness and relevance** through adaptive and informed decision-making
* Provide greater **assurance** regarding the management of significant risks
* Enable the exploration of **innovative solutions** to organizational and development challenges
* Inform effective and targeted 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.

1. 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.
2. 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)
* [Partner Capacity Assessment Tool (PCAT](https://popp.undp.org/document/partner-capacity-assessment-tool-pcat))
* [Partner Capacity Assessment on Prevention of Sexual Exploitation, Abuse and Harassment (PSEAH)](https://undp.sharepoint.com/teams/OHR-Portal/SitePages/PSEA/Tools-and-Resources.aspx?CT=1695733242947&OR=OWA-NT&CID=7ca87a59-5280-4137-97da-aa7232556b24&WSL=1&xsdata=MDV8MDJ8bmVzcmVlbi5hbGhlYnNoaUB1bmRwLm9yZ3wzNDgxMTE0YmU5MmQ0NjY2ZWUxYzA4ZGNiZTNkOTBjMHxiM2U1ZGI1ZTI5NDQ0ODM3OTlmNTc0ODhhY2U1NDMxOXwwfDB8NjM4NTk0NDIwNDQ0MTM2NjI2fFVua25vd258VFdGcGJHWnNiM2Q4ZXlKV0lqb2lNQzR3TGpBd01EQWlMQ0pRSWpvaVYybHVNeklpTENKQlRpSTZJazFoYVd3aUxDSlhWQ0k2TW4wPXwwfHx8&sdata=akNZVHZDMGhaSGZQcGtzSjM1YU5UWGljSXhQdk1OUkxoME5oc0N6eHVUbz0%3d&clickparams=eyAiWC1BcHBOYW1lIiA6ICJNaWNyb3NvZnQgT3V0bG9vayIsICJYLUFwcFZlcnNpb24iIDogIjE2LjAuMTc4MzAuMjAxMzgiLCAiT1MiIDogIldpbmRvd3MiIH0%3D" \l "sea-risk-assessment)
* [Direct Execution (DEX) Assessment](https://popp.undp.org/document/direct-execution-modality-dex-memo-and-capacity-assessment)
* [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](https://programmecriticality.org/Static/index.html)
* [UNSMS Security Policy Manual – Policy on Security Risk Management](https://policy.un.org/policy-doc/30312)
* [Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy](https://popp.undp.org/policy-page/anti-money-laundering-and-countering-financing-terrorism-policy)
* [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/Portfolio/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
* Transactional [Procurement Strategies and Procurement](https://popp.undp.org/node/1426) Planning

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

# ERM Methodology

1. The UNDP ERM methodology follows the International Organization for Standardization (ISO) 31000:2018 which consists of six key elements: 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:
2. At the project and/or portfolio level (i.e. Development Projects, Portfolios, Engagement Facilities, Development Services, Institutional and Development Effectiveness Projects, Multi-Country and South-South Projects);
3. at the programme/unit level (i.e. Country Office/Programme, Regional Bureaux/Programme, Central Bureaux/Programme);
4. at the corporate level.
5. UNDP 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 and assessment, treatment, monitoring, review and reporting. ~~D~~etailed information about UNDP’s ERM methodology is available in the Managing Risks Across UNDP Programming and Operations – Guidance Note[[2]](#footnote-3).

1. **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.
2. **Risk identification**: Potential risks across the **ERM risk categories** (see [Appendix 2](#_Appendix_2:_ERM)) should be considered to ensure that all relevant risks are identified and evaluated.
3. **Risk analysis**: The **ERM Criteria Model** (see [Appendix 3](#_Appendix_3:_ERM)) defines the five-point scale that is used to determine likelihood (i.e., 1-Not likely, 2-Low likelihood, 3-Moderately likely, 4-Highly likely, 5-Expected) and impact (i.e., 1-Negligible, 2-Minor, 3-Intermediate, 4-Extensive, 5-Extreme). At the programme/unit and corporate level, a more detailed analysis of consequences is applied to determine overall impact.

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** | | | | | |
|  | | *LOW MODERATE SUBSTANTIAL HIGH* | | | | | | |

1. **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. **Risk treatment:** For each High, Substantial or Moderate level risk, one or more risk treatment measures must be identified.
3. 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).
4. 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).
5. **Risk monitoring and review:** 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 portfolio and/or project management decisions, audits, and organizational performance.
6. **Risk 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.). In addition, **ad-hoc reporting** is often needed in crisis contexts or for High level risks that are time sensitive.
7. 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.
8. 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.

# Risk Ownership and Escalation Criteria

1. 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.
2. A risk is **escalated** when circumstances pertaining to the risk and/or treatment itself may exceed the authority/mandate or expertise of the Risk Owner. If one or more of the following escalation criteria is met, the Risk Owner must escalate the risk:

* Risk requires mitigation measures or resources that are beyond what the Risk Owner is authorized to decide;
* Risk cuts across, or may impact, multiple offices (e.g. reputational risk for the entire organization, which may require changes to corporate policies);
* 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 (SRM) and Social and Environmental Unit (SECU));
* A major security incident has occurred which has impacted UNDP personnel, facilities or programmes or the security environment has deteriorated requiring additional treatment measures and/or corporate support, e.g., security advice;
* When risk significance level is determined to be High and cannot be fully mitigated by the risk owner (e.g., high-risk projects and/or portfolio, risks with high reputational impact on the entire organization, engagement with oil and gas and extractives industry, partnerships with potential private sector entities with direct involvement in exclusionary criteria, countries in crisis level 2 and 3 , etc.);
* When risk significance level is determined to be High and outside of UNDP’s Risk Appetite levels/tolerance despite the mitigation measures put in place to reduce risk exposure.

1. 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, the response should be provided within 24 hours and it is acceptable to communicate escalation using phone or e-mail and update the Risk Register afterwards.
2. To ensure accountability and risk ownership, risk escalation and de-escalation must be formally done. In line with the accountability framework, escalation follows the applicable reporting line, i.e., from project and/or portfolios to programme to relevant Bureau (central/regional) and ultimately to the corporate level.

# ERM System

1. UNDP’s ERM system is designed to help UNDP personnel 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, organizational, 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.

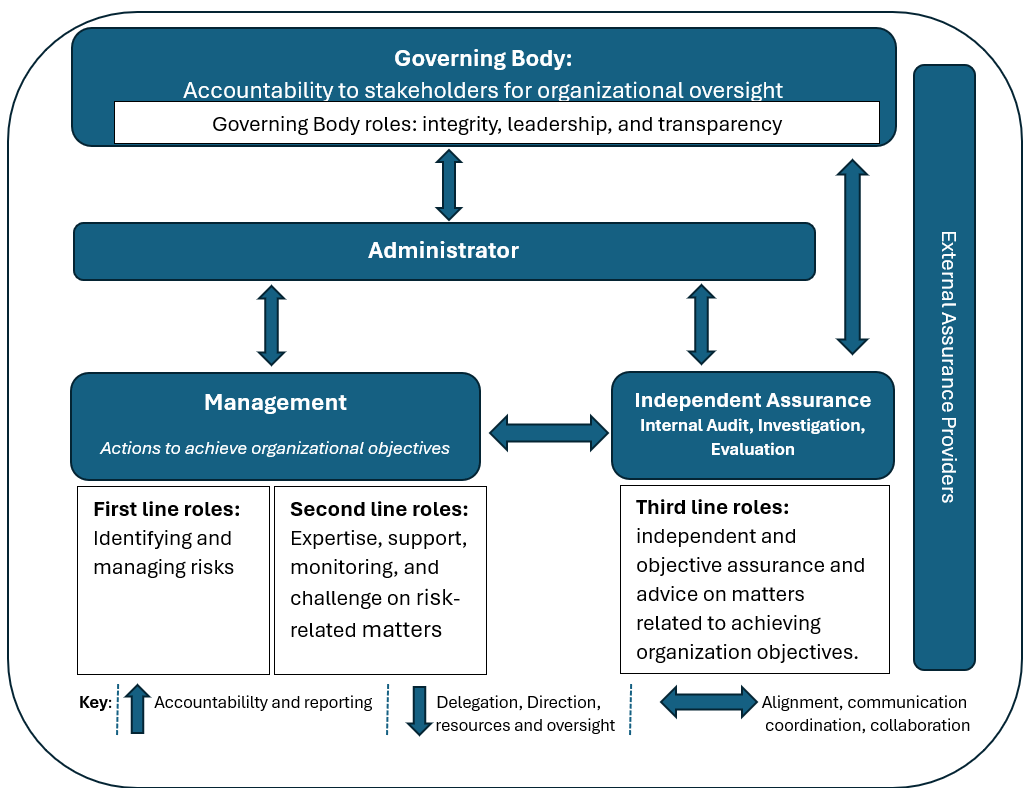
* The **project and/or portfolio Risk Register** reflects risks the project and/or portfolios is facing.
* The **programme/unit Risk Register** reflects common project/portfolio-level risks determined to be relevant for the programme, cross-cutting programmatic risks, and those related to unit-level operations (HR, procurement, security, fraud, etc.).
* The **corporate Risk Register** reflects risks that cut across the organization and may also include programme/unit-level risks determined to be critical for the entire organization (e.g., risk with reputational impact due to its nature or scale).

# Governance

## 5.1 Three Lines Model

1. The “Three Lines Model”[[3]](#footnote-4), supports effective risk management by introducing structured governance and processes, and clarifying roles and responsibilities. The relationship among the three lines is shown below.

**UNDP’s Three Lines Model in Risk Management:**



1. The key principles of the Three Lines Model are:
2. Governance of an organization. This requires appropriate structures and processes that enable i) accountability; ii) actions; and iii) assurance and advice.
3. Governing body roles. The governing body provides oversight and ensures appropriate structures and processes are in place for effective governance and that organizational objectives are responsive to the needs and priorities of recipient countries.
4. Management (First- and Second-lines roles). Management is responsible for achieving organizational objectives, including owning and managing risks (first line), and monitoring risks and providing support and expertise (second line).
5. Third line roles. This provides independent assurance and advice on the adequacy and effectiveness of organizational governance and risk management.
6. Third line independence. This ensures internal audit’s independence from the responsibilities of management to ensure its objectivity, authority and credibility.
7. Creating and protecting value. All roles work together, align activities and priorities through communication, cooperation and collaboration.

## 5.2 Key Roles and Responsibilities

1. **Governing Body:** UNDP Executive Board’s oversight roles and responsibilities were established by General Assembly resolution A/RES/48/162. It describes the responsibility of the Board as “*providing inter-governmental support to and supervision of the activities of each fund or programme in accordance with the overall policy guidance of the General Assembly and the Economic and Social Council, in accordance with their respective responsibilities set out in the Charter, and for ensuring they are responsive to the needs and priorities of recipient countries*”. The Executive Board, in exercising its own accountability and oversight responsibilities effectively at the strategic level, requires independent objective assurances and reports that decisions made at the policy level are implemented, resources are properly and ethically used for the purposes provided, and management is fulfilling the objectives (including effective risk management) set by the policymakers. The Executive Board reflects on key improvements to the ERM system as well as strategic risks of critical importance annually at the first regular session of the Executive Board as a joint item.
2. **Administrator:** As stated in the UNDP [Accountability Framework](https://popp.undp.org/document/accountability-system-policy), the Administrator is responsible for the operations of UNDP and is accountable to the Executive Board for all phases and aspects of the management and implementation of UNDP activities. The Administrator is accountable for providing organizational vision and direction following consultations with the Executive Board. The Administrator delegates authority to the UNDP Associate Administrator, Assistant Administrators (Bureau Directors), Resident Representatives and other unit heads for specific functions essential to their position in order to carry out the mandate of the organization. Accountability for the implementation of a systematic and organization-wide enterprise risk management framework (including policies and procedures) across UNDP rests with the Administrator and senior leadership of the organization, including the Chief Risk Officer/Associate Administrator.
3. **Management:** In line with the key principles of the Three Lines Model referenced in paragraph 21, management is responsible for achieving organizational objectives, including owning and managing risks (first line role), and monitoring risks and providing support and expertise (second line role).

### First Line Roles

1. All UNDP personnel have a role in risk management and the first line. Personnel are responsible for identifying and managing the risks that affect the achievement of objectives related to their area(s) of work within their delegated authority. They are accountable for ensuring compliance with various control activities and ensuring that these are adequately evidenced.
2. 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/document/accountability-system-policy).
3. At the corporate level, the **Executive Group** is accountable for ERM and for ensuring corporate decisions are risk informed.
4. At the programme/unit level:
   1. The **Directors of Regional/Central Bureaux[[4]](#footnote-5)** 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.
   2. For Country Offices/Programmes, the **Resident Representative (RR)/Head of Office** is ultimately responsible for ERM and is 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.
   3. 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.
   4. **Risk Focal Points** have advanced knowledge of risk management challenges affecting their office/bureaux; and serve as the main point of contact between UNDP staff, Heads of Offices, the Regional/Central Bureau and the Risk Committee Secretariat.
5. At the portfolio and/or project level, the **Portfolio and/or Project Assurance** function (e.g., UNDP Programme Officer) is responsible for ensuring the Risk Register is regularly updated and monitored for the portfolio and/or project, and that risk treatment measures are implemented. The Assurance function ensures risks are identified and managed by the project and/or portfolio manager.

### Second Line Roles

1. The second line is responsible for risk monitoring, advice, and technical support.
2. **Directors of Regional/Central Bureaux:** Directors of Bureaux oversee the overall management of risks and controls within their bureaux and are responsible for monitoring and ensuring that offices under their supervision keep their Risk Registers up to date, respond to risks appropriately, and report upwards in line as necessary.
3. **Risk Committee** (see [Appendix 5](#_Appendix_5._Risk) for the Risk Committee Terms of Reference) is an advisory group and a sub-committee of the Executive Group responsible for ensuring that the overall risk management framework is effective, relevant and applied corporately. The Risk Committee is also responsible for identifying corporate risks and for advising on potential treatment measures that can be adopted by risk owners. The Committee reviews and monitors the corporate risk register. It also recommends risks for escalation to the Administrator and provides advice/review on specific issues at the Administrator’s request. The Risk Committee is supported by the **Risk Committee Secretariat**, which sits in the Executive Office. 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 who may be invited to the Committee as needed.
4. **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.
5. **Technical experts** (e.g., Security, Procurement, Financial, Operations, Legal, Programme, Portfolio and Project Management, Social and Environmental Standards, media engagement and communications, etc.) play an important role in the second line, bringing technical expertise and support targeted to substantial and high-level risks. This also includes surge support and capacity to reinforce Country Offices facing high levels of risk to respond 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 Role

1. The third line role is independent assurance: internal audit, investigation and evaluation. UNDP’s **Office of Audit and Investigations (OAI)** carries out internal audits and investigations, and the Independent Evaluation Office (IEO)completes independent evaluations. They provide independent and objective assurance and advice on the risk management framework and practices in the organization and provide recommendations on ways to improve risk management.
2. **External Assurance providers:** In addition, the United Nations Board of Auditors (BoA) carries out the external audit of the accounts of the United Nations organization and its funds and programmes. The Board's report on UNDP's financial statements is a public document. It is presented to the General Assembly through the Fifth Committee and also to UNDP's Executive Board.

See [Appendix 4](#_Appendix_4._Summary) for a summary of risk management roles and responsibilities.

# Risk Management Culture

1. UNDP recognizes that mindsets and behaviors of individuals and offices inside the organization play a crucial role in the effective execution of risk management 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 and capacity building for strengthened risk management capacities.
* Key stakeholders are involved in all stages of the risk management process.
* Risk management is not approached as purely a compliance exercise.
* 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.

**Key Risk Indicators (KRIs)** are early warning indicatorsthat highlight when performance may be about to go outside the agreed risk appetite for a risk category and may cause unacceptable risk exposure.

**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, portfolio 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, portfolio, 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 the organization does to help 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, portfolio 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, portfolio 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 the response to negative events, and opportunity management, which is the 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 are mapped accordingly and reflected in Risk Register/QA system.

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

**Determining Likelihood (at Project, Portfolio, 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:**

***Portfolio and/or Project Level –***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact | Negligible | Minor | Intermediate | Extensive | Extreme |
| **1** | **2** | **3** | **4** | **5** |
| Description  (“If the risk materializes…”) | Negligible/no impact on portfolio and/or 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** |
| --- | --- | --- | --- |
| ***Governing Body Role*** | | | |
| **ExecutiveBoard** | | Provides inter-governmental support to and supervision of the activities of UNDP programme | * As stated in UNDP accountability framework, UNDP Executive Board’s oversight roles and responsibilities were established by General Assembly resolution A/RES/48/162. It describes the responsibility of the Board as “Providing inter-governmental support to and supervision of the activities of each fund or programme in accordance with the overall policy guidance of the General Assembly and the Economic and Social Council, in accordance with their respective responsibilities set out in the Charter, and for ensuring they are responsive to the needs and priorities of recipient countries”. |
| **Administrator** | | Accountable to the Executive Board for all phases and aspects of the management and implementation of UNDP activities. | * Responsible for the operations of UNDP and is accountable to the Executive Board for all phases and aspects of the management and implementation of UNDP activities. * Accountable for providing organizational vision and direction following consultations with the Executive Board. The Administrator delegates authority to the UNDP Associate Administrator, Assistant Administrators (Bureau Directors), Resident Representatives and other unit heads for specific functions essential to their position in order to carry out the mandate of the organization. * Accountability for the implementation of a systematic and organization-wide enterprise risk management framework (including policies and procedures) across UNDP rests with the Administrator and senior leadership of the organization, including the Chief Risk Officer/Associate Administrator. |
| ***First Line Roles*** | | | |
| **All UNDP Personnel** (at country, regional and headquarters levels)  *(Project, Portfolio, 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 area(s) of work within their delegated authority.  Personnel must communicate regularly to their supervisor(s) 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 at the level of their authority (i.e., for corporate risks, in their Business Unit or Country Office, or their project/portfolio, as relevant). * Escalate risk management issues and concerns beyond their authority as appropriate. |
| **Executive Group**  *(Corporate Level)* | The Executive Group is accountable for ERM implementation. | | * Ensuring corporate decisions are risk-informed and in compliance with UNDP policies and regulations. |
| **Regional and Central Bureau Directors[[5]](#footnote-6)**  *(Programme/Unit Level)* | As Head of Bureaux, accountable for enterprise risk management and risk-informed decision-making at the Bureau level, including identifying and managing risks impacting the achievement of objectives. | | * 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. * Ensure that the Programme Risk Registers for relevant Global/Regional Programmes and the bureau are regularly updated, and identified risks are managed, monitored and escalated as needed. 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. * Approve or reject risks which are escalated to the bureau. * Escalate risks to the Risk Committee as appropriate. |
| **Head of Offices (HoO) for Central Bureaux**  *(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, manage 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/or 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. * Manages risks escalated by projects and portfolios that are part of the country programme, as relevant.Escalates any risks that require attention of the bureau or the corporate risk committee as per the ERM policy. * Chairs the local portfolio and/or project appraisal committee to review the proposed portfolio and/or 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 portfolios and/or projects, and risks of high severity emanating from portfolios and/or projects and the various risks assessment tools, to ensure necessary and timely follow up action. * Review the proposed portfolio and/or 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 Bureaux 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/bureaux; 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 Bureaux 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 portfolio and/or project appraisal to provide inputs including formulating risk management plans during portfolio and/or project designs. * Ensures relevant colleagues and stakeholders from both programme and operations are consulted in the identification and management of risks for all portfolios and/or projects in the office/unit, and for the programme, if applicable. |
| **Portfolio and/or Project Assurance** (at country, regional and headquarters levels)  *(Portfolio and/or Project Level)* | The Portfolio and/or 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 portfolio and/or project and that risk treatment measures are implemented. |
| ***Second Line Roles*** | | | |
| **Risk Committee** | The Risk Committee is an advisory group and 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 in their capacity as Chief Risk Officer. * Oversight of UNDP risk management policies and practices framework. * Focus on strategic corporate risks that are escalated to and/or identified by the committee. * Identify corporate risks and advise on potential treatment measures that can be adopted by risk owners, drawing on insights of relevant technical experts and other review mechanisms such as the Private Sector Due Diligence Committee, and report to the EG. * Review and monitor the corporate risk register. * Recommend risks to be escalated to the Administrator and provide advice/review on specific issues at the Administrator’s request. * 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 for Risk Committee meetings. * Liaise with Bureaux regarding relevant background materials. * Ensure proper documentation of Risk Committee discussions. * Conduct the analysis of aggregated risk registers as part of corporate risk analysis. * Record and present escalated risks for Risk Committee deliberations. * Facilitate the presentation of evidence relating to critical risks of strategic importance. * Ensure proper recording of risks in the corporate risk register. * 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 proactive, 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 portfolio and/or project 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. |
| **Regional and Central Bureau Directors** | As Heads of Bureaux, monitor and oversee the overall management of risks and controls within their bureaux, including COs/BUs. | | * Ensure COs/BUs under their supervision keep their Risk Registers up to date, respond to risks appropriately, and report upwards in line as necessary. * Monitor risks and risk treatments and ensure that risks are within the appropriate risk appetite levels * Provide consultative, technical and resource assistance to escalated risk from offices. * Chair bureau risk discussions to review risk information including indicators and appetite metrics and follow-up on mitigation measures. |
| **BMS and BPPS**  **Directors** | 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, Portfolio and Project Management, Social and Environmental Standards, Media engagement and communications, 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 Role*** | | | |
| **Office of Audit and Investigations (OAI) and Independent Evaluation Office (IEO)** | Provide independent and objective assurance and advice | | * Provide independent and objective assurance and advice on the risk management framework and practices in the organization and provide recommendations on ways to improve risk management. |
| ***External Assurance Providers*** | | | |
| **UN Board of Auditors** | The United Nations Board of Auditors (BoA) carries out the external audit of the accounts of the United Nations organization and its funds and programmes. | | * Conducts external audits and reports on UNDP's financial statements through a public document, which is presented to the General Assembly through the Fifth Committee and to UNDP's Executive Board. |

# Appendix 5. Risk Committee Terms of Reference

### Background

Enterprise risk management (ERM), including the strategic aspect of Security and Crisis Management and Business Continuity Management, 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, the Risk Committee is an advisory group chaired by the Associate Administrator to oversee the overall implementation, and use, of the risk management framework in UNDP. The Risk Committee is a subcommittee of the EG. It recommends risks to be escalated to the Administrator and provides advice/review on specific issues at the Administrator’s request. The Risk Committee reports back to the EG on the framework on an as needed basis.

### Duties and Responsibilities

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

1. ***Identifying, Reviewing and Analyzing Corporate Risks***

Under this responsibility, the committee will identify, review, and deliberate corporate risks and risk management/treatment strategies, and where necessary, propose amendments or revised strategies. The Committee shall focus on strategic corporate risks that are identified by the committee or escalated to the committee, including risks escalated from discussion in other respective forums. (e.g., the OPG, SMG, Crisis Board, etc.).

1. Escalated risks from other corporate mechanisms;

The chair and the member of the Committee can bring to the table risks that are identified and escalated to the Committee through the different corporate mechanisms, e.g.:

* The *Organizational Performance Group (OPG)* for high risks related to institutional and/or operational matters related to organizational performance, including the top audit risks priorities;
* The *Crisis Board*, for high risks related to a particular country programme in on-going crisis;
* The *Security Management Group* for high risks related to staff safety and security as well as business continuity in Headquarters;
* Private Sector Due Diligence Committee, for escalated risky partnerships with the private sector; and
* Other corporate mechanisms as relevant.

1. Analysis from aggregated Risk Register;

On an annual basis, risks analysis from bureau risk entries in the aggregated risk registers 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. Corporately identified risks

Risk Committee members, along with relevant technical experts, will proactively present evidence on corporate risks to the Risk Committee with a view to enable identification of critical risks of strategic importance.

1. Escalated risks from bureau and units

In line with the criteria for risk escalation, all risks that are escalated to the corporate level will be reviewed electronically, especially for escalated project risks that can be handled via e-review. When required, escalated risks can 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), Security and Crisis Management ), 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 updates to 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)[[6]](#footnote-7) 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 reports back to the EG on an as-needed 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 regard, the permanent membership of the Committee is as follows:

* 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 Crisis Bureau;
* 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 an advisory group and is a sub-committee to the Executive Group. The relationship with other corporate decision-making structures can be depicted as follows:

**RC: RISK ANALYSIS, EVALUATION, RECOMMENDATION AND MONITORING**

The Risk Committee reviews, analyses and provides advice about corporate risks that are recommended for escalation through the different corporate mechanisms and data sources (e.g. OPG, SMG, Crisis Board, Risk Register, etc.) as well as through risk analysis by different Bureaux and/or technical experts. 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 four times a year. On an 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 agenda for Risk Committee meetings can include topics such as:

* Review the effectiveness of the ERM implementation (including the policies, procedures, learning and other tools);
* Identify, 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;
* Review risks escalated by other mechanisms and/or bureaux;
* Any other business

1. ***Risk Committee Secretariat***

The Risk Committee is supported by a secretariat (EXO/CPU) to assist the chair and Committee members in effective and efficient management of committee meetings. This includes:

* Preparing agenda for committee meetings;
* Liaise with Bureaux regarding relevant background materials;
* Conduct the analysis of aggregated risk registers as part of corporate risk analysis;
* Record and present escalated risks for committee deliberations;
* Facilitate the presentation of evidence relating to critical risks of strategic importance.
* Ensure proper recording of risks in the corporate risk register; and
* Any other tasks as assigned by the chair of the Committee.

# Appendix 6. Procedures

Procedures for Managing **Portfolio and/or Project-Level Risk** (Country, Regional or Global Portfolios and/or 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 Portfolio and/or Project Board and other stakeholders/partners informed on RM processes at the portfolio and/or project level. |
| **2- Scope, context and Criteria** | Portfolio developer, Project Developer,  Portfolio Manager, or Project Manager | [Project Document Template](https://popp.undp.org/node/1131)  [Portfolio Document Template](https://popp.undp.org/document/portfolio-document-template)  [Portfolio and/or Project Risk Register](https://popp.undp.org/node/326) | Integrated in Programme and/or Portfolio Document, Project Document, Multi-Year Work Plan |
| **3- Risk Assessment:**  Identification of Risks | Portfolio developer, Project Developer,  Portfolio Manager, or Project Manager | [Portfolio/Project Risk Register](https://popp.undp.org/node/326) | Assess risks during Portfolio/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 portfolio/project objectives. |
| Risk Analysis | Portfolio developer, Project Developer,  Portfolio Manager, or Project Manager | [Portfolio/Project Risk Register](https://popp.undp.org/node/326) | Analyze likelihood and impact of the portfolio/project risks by applying the ERM Criteria Model and record in Risk Register. |
| Evaluation of Risk | Portfolio Manager and/or Project Manager | [Portfolio/Project Risk Register](https://popp.undp.org/node/326) | Evaluate each portfolio/project risk to determine which risks can be accepted and which risks require a priority treatment in order to meet portfolio/project objectives and avoid harm. |
| **4- Risk Treatment** | Portfolio/Project Developer or  Portfolio/Project Manager | [Portfolio/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 portfolio/project design, prior to portfolio/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 | [Portfolio/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 portfolio/project. Update Risk Register once a year at a minimum. |
|  |
| **6-Risk Recording and Reporting** | Portfolio/Project Manager | [Portfolio/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 portfolio/project reporting cycle, once a year at a minimum. Portfolio/Project risks presented to the Portfolio/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 portfolio/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 prioritized, 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** | | | |
| **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)  [Portfolio Document Template](https://popp.undp.org/document/portfolio-document-template)  [Unit Risk Register (Quantum+)](https://undp.lightning.force.com/lightning/page/home) | 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 Bureaux 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) | 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 publication of this standard was last reviewed in 2023 and confirmed to remain current. Source: <https://www.iso.org/standard/65694.html> [↑](#footnote-ref-2)
2. <https://popp.undp.org/document/managing-risks-across-undp-programming-and-operations-guidance-note> [↑](#footnote-ref-3)
3. https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/ [↑](#footnote-ref-4)
4. In addition, the UNV Executive Coordinator and UNOSSC Director for UNV and UNOSSC respectively. [↑](#footnote-ref-5)
5. In addition, the UNV Executive Coordinator and UNOSSC Director for UNV and UNOSSC respectively. [↑](#footnote-ref-6)
6. 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-7)