UNDP Enterprise Risk Management (ERM) Policy

Effective Date – 13/03/2019

Policy Owner: BMS/BPPS

Approved November 2018

What is New

The revisions to the ERM policy focus on enhancing the following:

- ✓ Importance of cultivating a ***risk culture*** within the organization to enable responsible risk-taking and risk-informed decision-making
- ✓ ***Unity in the approach and methodology*** used for risk management across programming and operations (including through a common Risk Register)
- ✓ Fostering ***opportunity management***, foresight, and innovation, rather than an approach that focusses only on avoiding harm and reacting to issues as they arise.
- ✓ Greater ***alignment between risk categories and programming quality criteria***, ensuring risk management and quality assurance go hand-in-hand.
- ✓ ***Maintaining a simplified risk assessment*** at the project level, while ensuring alignment with ERM methodology.
- ✓ Importance of ***aligning risk reporting to the existing reporting cycles*** within the organization
- ✓ Introduction of the "***Three Lines of Defence***" for risk management and governance

Specific changes include:

ERM Policy 2016	Change
Policy **Owner**: BMS	***Changed*** to shared ownership of BMS and BPPS, ensuring an approach that brings together programming and operations.
Policy **Structure and Language** process heavy	***Changed:*** Adjusted language to be less process heavy and more focused on defining the standards for quality ERM.
Terms and Definitions	***Clarified*** definitions related to programmatic risk and separated definitions from policy text.
Risk Register in IWP and separate Project Risk Log in Atlas	***Changed:*** Alignment between Atlas project risk log and IWP Risk Register. Proposal for fully integrated risk information system.
ERM Criteria Model required across all levels of risk	***Simplified*** ERM Criteria Model is introduced for projects, to be built into Risk Register.
Lack of clarity on **Risk Assessment** (identification, analysis, evaluation) process at the project level	***Clarified*** the key elements of quality Risk Assessment, ensuring linkages with existing prescriptive processes such as Theory of Change, SES, HACT, security assessments, etc. ***Clarified*** requirements ensuring a consultative process, engaging key internal (e.g. programming and operations) and external stakeholders. ***Clarified*** risk matrix to ensure aligned risk categorization across all levels.
ERM **Risk Categorization**	***Changed:*** 8 risk categories, introducing Safety and Security as a new category. ERM categories to be mapped to programming quality criteria so that risk management and programming quality can be more closely linked.
Broad definition of risk but narrow interpretation in the policy focusing on **negative effects** of risk	***Introduced:*** consideration of positive effects of risks and opportunity management through risk treatment and the criteria model.
Risk Reporting requirements unclear at the project level	***Clarified:*** project risk reporting is aligned with project reporting cycles (minimum once a year).
ERM **governance** structures not clearly defined	***Introduced:*** the three lines of defence for effective risk management, consistent with the UN Risk Management, Oversight and Accountability Model
ERM **Procedures**	***Introduced:*** a table of ERM Procedures, following the POPP template to clarify process and roles/responsibilities.

Table of Contents

1. 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 as the effect of uncertainty on organizational objectives, which could be either positive and/or negative (ISO 31000:2018; see Appendix 1 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 approach to 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:

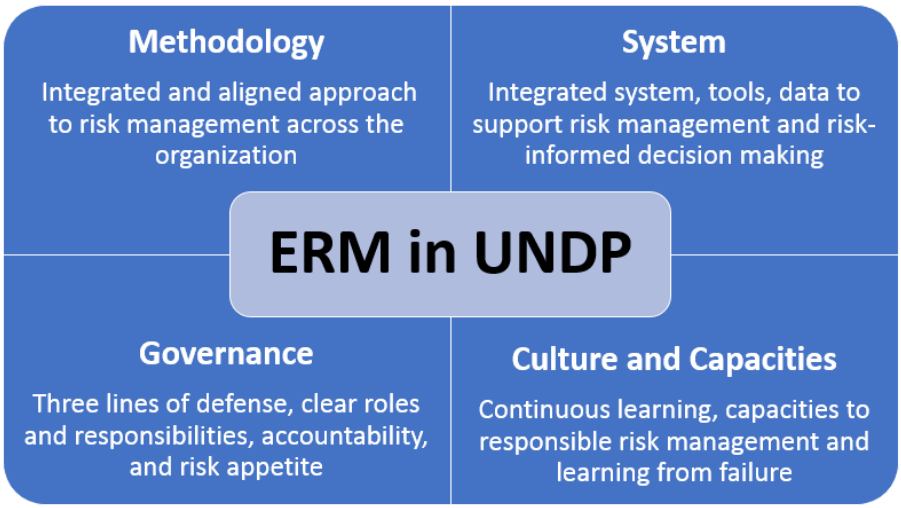
- Increase **programme effectiveness and relevance** through adaptive and informed decision-making
- Provide greater **assurance** regarding the management of significant risks
- Enable the exploration of **innovative solutions** to organizational and development challenges
- Inform effective and targeted 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 UNDP personnel, 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 UNDAF process and through joint programming (refer to UNDAF 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:

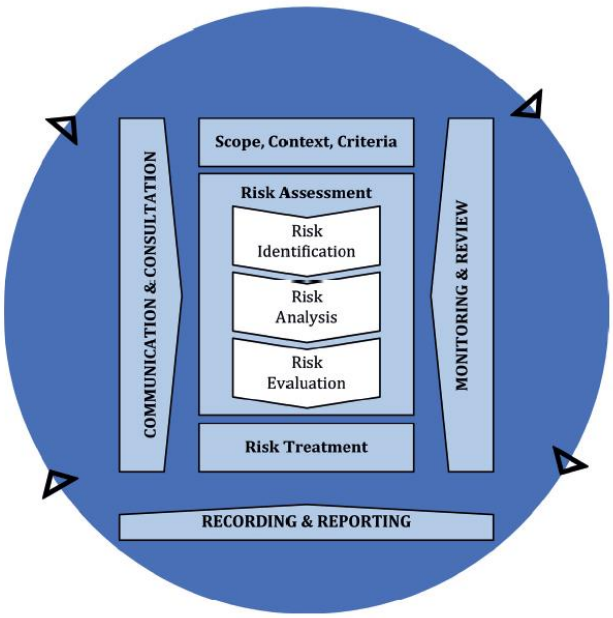
- Harmonized Approach to Cash Transfer
- Capacity assessments (of partners and UNDP)
- UNDP Anti-Fraud Policy
- UN Programme Criticality Framework
- UN Security Risk Management (SRM) Policy
- Business Continuity Management
- UNDP Policy on Due Diligence and Partnerships with the Private Sector
- Programme/Project Quality Assurance
- Social and Environmental Standards and Screening Procedure
- Theory of Change
- Audits and Evaluations
- Procurement Ethics, Fraud and Corrupt Practices Policy
- Procurement Strategy and Procurement Planning

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



2. 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:



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

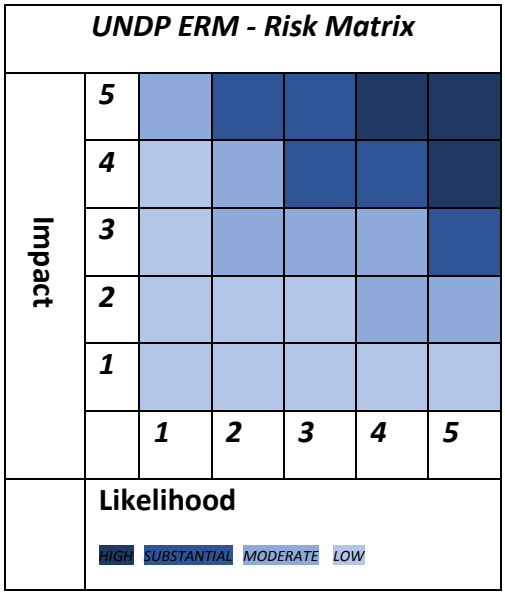
Risk Analysis

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) 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.

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, 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:

(a) 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 IWP Risk Register.

(b) 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.

(c) At the project level the project 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 Defence

The "Three Lines of Defence"[1] support more effective risk management by introducing structured governance and oversight that clarifies and segregates roles and responsibilities based on the following:

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

First Line of Defence

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

- At the corporate level, the **Executive Group** is accountable for ERM and ensuring corporate decisions are risk-informed.

[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.

- At the programme/unit level:

    - The **Directors of Regional/Central Bureaux** are accountable for ERM and risk-informed decision-making at the Bureau level and are accountable to the Administrator. Bureau Directors ensure the Risk Registers for relevant Global/Regional Programmes are regularly updated, identified risks are managed and escalated as needed. Directors of Bureaus are also responsible for ensuring that offices under their supervision (e.g. Country Offices for Regional Bureau and Liaison Offices for BERA) keep their Risk Registers up to date, respond to risks appropriately, and report upwards in line as necessary.

    - For Country Offices/Programmes, the **Resident Representative/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.

- 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 Defence

The second line of defence is responsible for risk oversight, monitoring and technical support. This is a key function of UNDP's **Risk Committee**, 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 Committee is chaired by the Associate Administrator 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).

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 defence, bringing technical oversight, knowledge, and support targeted to SUBSTANTIAL and HIGH-level risks.

The second line of defence 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 Defence

The third line of defence is the independent assurance and audit function. UNDP's Office of Audit and Investigations (OAI) as well as UN mechanisms, such as the Board of Auditors (BOA and Joint Inspection Unit (JIU), play this role.

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 budget 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

1.Social and Environmental	2. Financial	3.Operational	4.Organizational	5. Political	2.Regulatory	7. Strategic	8. Safety and Security
1.1. Human rights 1.2. Gender 1.3. Biodiversity and use of natural resources 1.4. Climate change and disaster 1.5. Community health and safety 1.6. Labour conditions/standards 1.7. Cultural heritage 1.8. Rights of Indigenous Peoples 1.9. Displacement and resettlement 1.10. Pollution and resource efficiency 1.11. Stakeholder engagement 1.12. Sexual exploitation and abuse	2.1. Cost recovery 2.2. Value for money 2.3. Corruption and fraud 2.4. Fluctuation in credit rate, market, currency 2.5. Delivery	3.1. Alignment with national priorities 3.2. Responsiveness to lessons learned and evaluations 3.3. Leadership & management 3.4. Flexibility and opportunity management 3.5. Synergy potential (linking with other initiatives as relevant) 3.6. Reporting and communication 3.7. Partnership 3.8. Capacity development of national partners 3.9. Engagement of national partners in decision-making 3.10. Transition and exit strategy	4.1. Governance 4.2. Monitoring 4.3. Independence and quality of evaluation 4.4. Knowledge management 4.5. Grievances 4.6. Due diligence of private sector partners 4.7. Human Resources 4.8. Budget availability and cash flow 4.9. Internal control 4.10. Procurement 4.11. Innovating, piloting, experimenting,	5.1. Government commitment 5.2. Political will 5.3. Political instability 5.4. Change/ turnover in government	6.1. Changes in the regulatory framework within the country of operation 6.2. Changes in the international regulatory framework affecting the whole organization 6.3. Deviation from UNDP internal rules and regulations	7.1. Theory of change 7.2. Alignment with UNDP Strategic priorities 7.3. Capacities of the partners 7.4. Roles and responsibilities among partners 7.5. Code of conduct and ethics 7.6. Public opinion and media 7.7. Synergy with UN / Delivery as One	8.1 Armed Conflict 8.2 Terrorism 8.3 Crime 8.4 Civil Unrest 8.5 Natural Hazards 8.6 Manmade Hazards

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 1	Low likelihood 2	Moderately likely 3	Highly likely 4	Expected 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 1	Minor 2	Intermediate 3	Extensive 4	Extreme 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 1	Minor 2	Intermediate 3	Extensive 4	Extreme 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