# Managing Risks Across UNDP Programming and Operations

GUIDANCE NOTE

September 2019

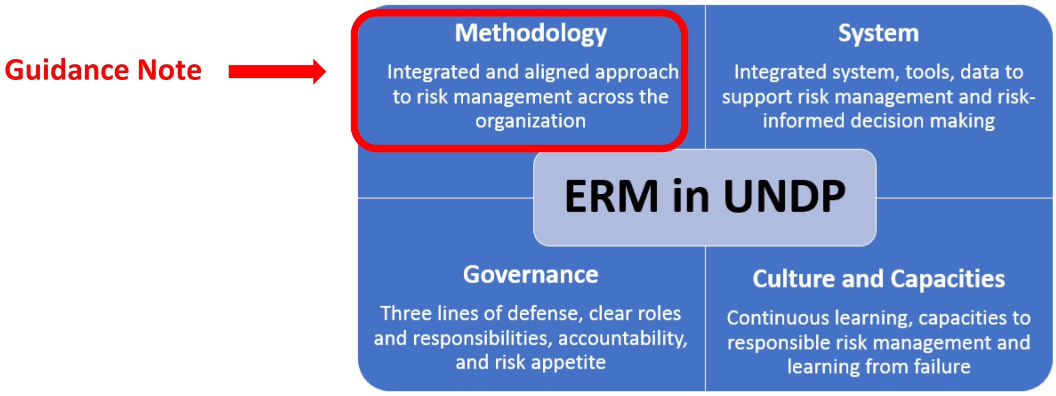
## Table of Contents

# INTRODUCTION

This guidance note aims to clarify UNDP's approach to Enterprise Risk Management (ERM) in practical terms. It is intended for both programming and operational staff to ensure a shared understanding of UNDP's risk management methodology across all levels and types of risk. More detailed guidance and tools related to particular types of risk are supplemental to this note and brought together in UNDP's Risk Management Platform (info.undp.org/erm).

The guidance note starts with the basics of what risk management is and why it is important. It then breaks down the steps of the UNDP ERM methodology. The guidance has seven modules, each of which is organized around a set of practical questions to guide users to the information they are seeking.

**DIAGRAM 1: Pillars of ERM in UNDP**




The seven sections of this guidance include the following:

1. What is risk management and why it is important
2. Establishing scope, context, and criteria
3. Risk Assessment
4. Risk Treatment (and escalation)
5. Risk Monitoring and Review
6. Risk Recording and Reporting
7. Risk Communication and Consultation

# 1 What is Risk Management and Why It Is Important

## 1.1 What is risk?

UNDP embraces the risk definition proposed by ISO 31000:2018 that is, *risk is the effect of uncertainty on objectives*. There are several important considerations about risks to note.

- ***Effect** can be positive or negative:* Many people associate "risk" only with negative consequences; however, potential positive consequences should also be identified and managed. The effect might change over time and that certain changes might have both negative consequences and positive consequences.

**_RISK =_**
**EFFECT of UNCERTAINTY on OBJECTIVES**

- ***Uncertainty** relates to our limited knowledge of the future*: Therefore, the identification of risks considers potential change from the expected or a future event that might have an effect on our objectives. This requires a forward-looking approach while having a good understanding of the context.
- ***Risks are attached to objectives***: Not all uncertainties are risks because not all uncertainties matter to us, only those that are related to our objectives. Note that risks are socially and contextually constructed; there are differences in objectives and concerns across various risk stakeholders. Therefore, when discussing risks always put the shared objectives at the core of the risk identification discussion.

## 1.2 What is risk management?

Embracing and navigating through uncertainties is at the core of risk management. Those uncertainties might impact the relevance of our objectives, the time within which we plan to reach our objectives, the budget within which we expect to realize our objectives, etc. By understanding these uncertainties through mapping and scanning potential events, their causes and impacts, we can ***improve our performance by*** **maximizing gains while avoiding unnecessary losses**.

The ultimate **purpose of risk management is to inform decision-making** at all levels: across project, programme, and all organizational levels. Risk management helps us to anticipate the future by (1) understanding the context (2) thinking about what might happen, (3) understanding the scope and scale of the consequences of an event in the future, and (4) making decisions that would help us to minimize negative impacts and maximize positive ones.

UNDP takes an integrated approach to risk management, with a unified approach across all types and levels within the organization. Risks are considered in their broad variability, with different risks related to programming and operations, from both internal and external contexts. It is also an inclusive process with the different stakeholders whose engagement in understanding and owning risks is critical for the success of any intervention and achieving our objectives.

## 1.3 Why is risk management important?

Effective risk management enables smart risk-taking and adaptive management. It builds confidence to be innovative and creative while anticipating and managing risks.

UNDP continues to work together with its national and international partners in highly complex and constantly changing context. We must take informed choices:

- To ensure that ***programmes are effective and relevant***
- To find more ***innovative solutions*** to deliver higher impact
- To ***allocate resources*** where they are most needed
- To be ***accountable for the results produced*** considering internal and external constraints
- To safeguard ***people and the environment***
- To manage ***safety and security*** risks to UNDP personnel, premises and assets, i.e. reduced to an acceptable level.

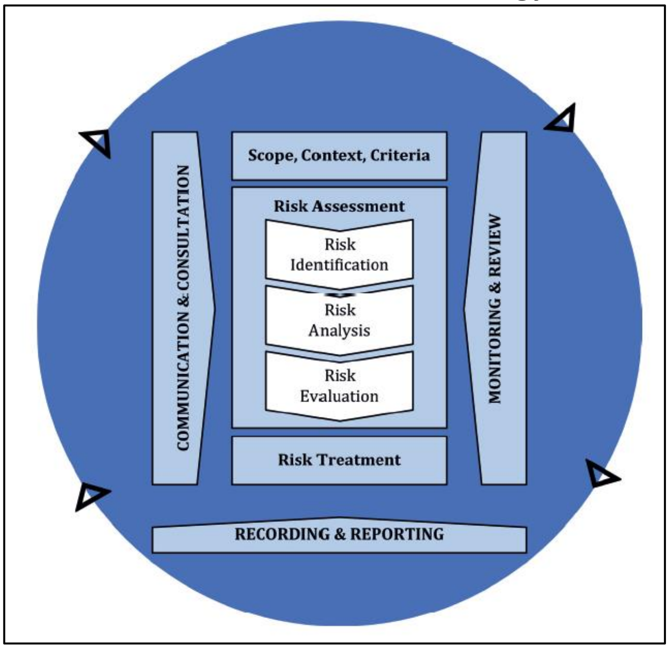
> ***"A decision that does not involve risk, probably is not a decision"***
>
> *Peter Drucker*

All these are critical for the reputation of UNDP as a value-driven and risk-informed organization, that takes decisions that are the most optimal given all the internal and external limitations and uncertainties. Only then UNDP and its partners can be assured that the chosen pathway towards sustainable development and its implementation is the guaranteed gateway to the expected results.

## 1.4 What is the UNDP ERM Approach?

UNDP's ERM Policy (2018) is based on an integrated risk management approach. The methodology is in line with the ISO 31000:2018:
(a) establishing scope, context, criteria;
(b) risk assessment;
(c) risk treatment;
(d) monitoring and review; and
(e) recording and reporting; communication and consultation (see Diagram 2).

**DIAGRAM 2: ERM Methodology**




The ERM methodology is applied across the whole organization at different levels:

- ***Project level*** (i.e. Development Projects, Engagement Facilities, Development Services, Institutional and Development Effectiveness Projects, Multi-Country and South-South Projects);
- ***Programme /Unit level*** (i.e. Country Office/Programme, Regional Bureaux/Programme, Central Bureaux/Programme);
- ***Corporate level:*** organization as a whole.

Sections 2-7 of this guidance provide further details on the various steps of the ERM process. Annex 2 provides visualization of the ERM processes according to organizational levels.

# 2 Establishing the Scope and Context

## 2.1 What is the purpose of this stage?

Understanding the evolving internal and external context in which we operate is the first step for effective risk management and navigating uncertainties. This helps ensure a wide field of vision to scan for potential opportunities and hazards on the way to our objectives.

## 2.2 Which contextual factors should be considered?

> ***The most basic form of human stupidity is forgetting what we are trying to accomplish.***
> ***-Friedrich Nietzsche***

Internal Context: What are your objectives? What is the duration? Who are the key internal stakeholders? What resources and capacities are in place? What are the governance mechanisms and institutional arrangements? What are the relevant legal and policy requirements? Are their institutional change processes underway that may affect your objectives?

External Context: Who are the key external stakeholders? What is the external legal and regulatory framework? What are the key factors and trends that are relevant to the objectives? (consider trends and factors related to geography, economy, climate, natural hazards, political, security, poverty level, corruption, criminality, etc.). Various data sources and evidence can be drawn from. For example, UNDP's Crisis Risk Dashboard.

## 2.3. What needs to be recorded?

There is no need to record this stage. For programmes and projects, key contextual factors should be captured in the programme or project document. What is important is for teams to be familiar with relevant contextual factors and to keep an eye on how they evolve over time and how they may affect objectives.

# 3 Risk Assessment

The risk assessment process is composed of three steps: (1) risk identification, (2) risk analysis, and (3) risk evaluation.

### Risk Identification

## 3.1 What is the purpose of risk identification?

> ***Risks that are not identified are not managed!***

Risks that are not identified won't be managed. Knowing and understanding relevant risks ensures smarter decision making for the achievement of objectives, avoiding pitfalls and seizing opportunities along the way. Failing to acknowledge or identify risks can often lead to poor planning, decision making, unexpected costs and delays, and missed opportunities.

## 3.2 How to identify risks?

Risk identification is a constant process involving foresight, horizon scanning and stakeholder engagement. To get started, the following steps and tools can facilitate the risk identification process:

- ✓ Consider the context: The contextual analysis, identifying key trends and issues, hazards and opportunities, provides a key source of evidence to inform the identification of risks. Note that the context is always changing so continuous risk identification requires a close eye on the changing context.
- ✓ Review ERM Risk Categories: UNDP has identified risks categories that are critically important for performance (see Table 1). These categories include various elements of social and environmental, financial, operational, organizational, political, regulatory, strategic, safety and security risks. Not all types of risks might be relevant but reviewing the categories and sub-categories during the risk identification process helps ensure all types of risks are considered. Examples of each category of risk you can find in Annex 2.
- ✓ Use risk screening and due diligence tools: UNDP has many risk screening tools that help us scan for risks that otherwise may be missed. For example, the HACT, Security Risk Analysis, Social and Environmental Screening Procedure, and Private Sector Due Diligence tool. However, when these tools are approached as a check-the-box exercise, the risks are often overlooked.

> ***High risk is not necessarily bad!***
> It is often high risk contexts where UNDP is most needed and where transformative results become possible.

- ✓ Review the Risk Register/Dashboard: The Risk Register and related Dashboard is a good place to scan previously identified risks and re-assess their relevance. Some risks may be common across several projects and could have an impact on the programme level, and vice versa. To identify project level risks, it is critical to understand the programme context and risks and not approach project risks in isolation.
- ✓ Engage stakeholders: Risk identification requires approaching the problem from multiple perspectives. It cannot be the job of one person. Potential risks need to be explicitly discussed with key stakeholders including internal programme and operational experts, external experts and partners, and stakeholders who may be affected by the activities.

## 3.3 How to describe risks?

A good risk description is based on an initial analysis that is sufficiently detailed to inform appropriate actions. According to the ERM policy, the risk description consists of the following:

a. event (i.e. deviation from expected or planned, an uncertain event that might or might not happen),
b. causes of such an event), and
c. impact on the objective(s) should the risk materialize.

The description should also reflect where the uncertainty lies, e.g. noting if the event, cause, or impact might or might not happen.

Note that the impact can be related to the specific objectives of the intervention or impacts to people and the environment that may result from our activities, thereby affecting UNDP's overall objectives and mandate.

## Risk Analysis

### 3.4 What is the purpose of risk analysis?

After risks are identified, each risk needs to be analyzed from the perspective of the *likelihood* of it happening and the *impact* (positive or negative) it might cause - if and when it happens. UNDP ERM methodology requires that both impact and likelihood are measured on a 5-point scale as defined in the ERM Policy, **Criteria Model** (see Table 2 of ERM Policy).

**Determining Likelihood and Impact**
The application of the Criteria Model in the risk analysis process is often not a precise science. Available information and evidence need to be considered, including 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 for any adjustment. In cases of potential significant risk where very little information is available, a full risk analysis should be conducted. Discussions with experts and key stakeholders is also an essential part of risk analysis. In many cases, there still remains some degree of professional judgement, which is why risk analysis is an ongoing process to ensure risk levels are adjusted as new information becomes available.

### 3.5 How to determine LIKELIHOOD (L)?

The ERM Policy identifies several degrees of likelihood on 5-point scale with some guiding criteria:

| Likelihood | Not likely<br>1 | Low likelihood<br>2 | Moderately likely<br>3 | Highly likely<br>4 | Expected<br>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% |

Available historical data, forecasting data and trend analyses may be helpful in determining likelihood.

## 3.6 How to determine IMPACT (I)?

*Impact* is also ranked on a 5-point scale. The determination of Impact should be informed by discussions with experts, stakeholders (particularly those who may be affected), available risk assessments and data. The ERM Policy identifies several types consequences that should be considered when determining overall impact. These consequences are those related to development results, operations, compliance, safety & security, and reputation. While consideration of these various consequences is helpful for all levels and types of risk, UNDP applies a **simplified analysis of *Impact* at the Project level**:

| Impact | Negligible<br>1 | Minor<br>2 | Intermediate<br>3 | Extensive<br>4 | Extreme<br>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 50% 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. |

At the **Programme/Unit and Corporate levels, each of the different consequences needs to be assessed using the ERM Criteria Model**. The overall *Impact* of a risk is then based on the highest level of impact across the different consequences (e.g. if one of the consequences has an impact of 5, then the overall Impact for that risk is 5).

<table>
<tr><th colspan="2">Impact</th><th>Negligible<br>1</th><th>Minor<br>2</th><th>Intermediate<br>3</th><th>Extensive<br>4</th><th>Extreme<br>5</th></tr>
<tr><td rowspan="2">Description of Consequences</td><td rowspan="2">Financial (absolute and relative)</td><td colspan="5">Estimated range in USD, 3 numbers:<br>• Maximum (highest level of potential deviation, +/-))<br>• Likely (best guess)<br>• Minimum (lowest level of potential deviation, +/-) )<br>which, based on best guess figure, corresponds to:</td></tr>
<tr><td><5 % deviation from applicable budget</td><td>5-20 % deviation from applicable budget</td><td>20-30% deviation from applicable budget</td><td>30-50% deviation from applicable budget</td><td>>50% deviation from applicable budget</td></tr>
</table>

| | | | | | | |
|---|---|---|---|---|---|---|
| | **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 |

**Calculating Financial Consequence**

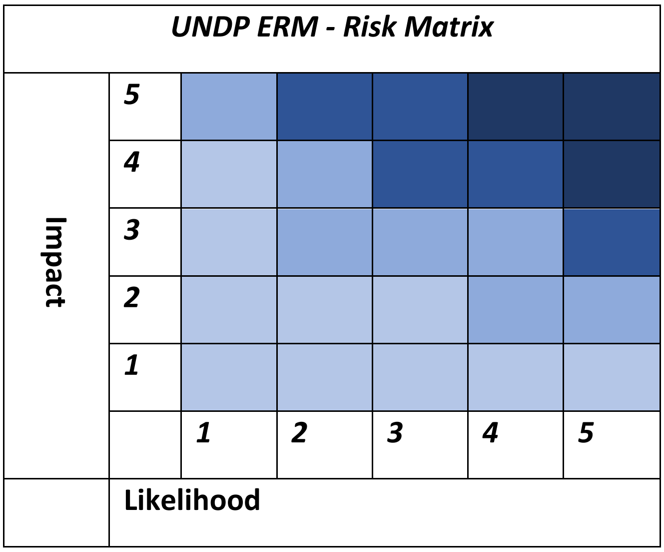
Quantification of the financial consequence is not a straightforward exercise. Qualitative data analysis as well as in depth understanding of the context are important factors when calculating risk's financial loss. These include key stakeholders' tolerance to identified risks, source of risk and when it occurs, as well as its likelihood and impact. According to our ERM policy, financial consequence is defined as "the amount of fund that the organization needs to commit to rectify the situation once the risk materialized." In that regards, financial consequence is not: 1) The "opportunity loss" that the organization suffers when the risk materializes; for instance, if a risk undermines the possibility to mobilize resources, the realization of the risk will impact the possibility to achieve development results, but it will not translate in a financial impact equal to the resources which were not mobilized. 2)The cost of prevention and risk mitigation measures; 3)- Monetized amount of loss of productivity (e.g. staff time, running cost, etc.); or 4) The loss generated from exchange rate from non-core rescores.

Financial impact is NOT about the "opportunity loss" that the organization suffers when the risk materializes. For instance, if a risk undermines the possibility to mobilize resources, the financial impact DOES NOT equal to the resources which were not mobilized.

**Examples of Financial loss quantification can be found here**

## 3.7 How to determine risk SIGNIFICANCE?

Once the Impact and Likelihood are determined, the overall risk *Significance* (Low, Moderate, Substantial or High) is identified using the ERM risk matrix:




Key: ***HIGH*** ***SUBSTANTIAL*** ***MODERATE*** ***LOW***

## 3.8 When is additional risk analysis required?

Risks that are HIGH significance require a thorough risk analysis. This may require relevant expertise (internal or external) to further assist in the risk analysis. Where possible, risk analysis should look across multiple risks to understand linkages and tradeoffs. For example, and Environmental and Social Impact Assessment of a project can help to look across environmental and social risks to ensure an integrated approach.

Further risk analysis may also be needed when there is a lack of information to be able to assess likelihood and impact or even identify potential risks.

## Risk Evaluation

### 3.9 What is the purpose of risk evaluation?

The *risk evaluation process is about* ***risk prioritization***. Out of all risks that have been identified and then analyzed, the team decides on which risks can be accepted those that should be considered priority for response.

Note that High level risks should not necessarily be avoided (unless there is a potential for harm, fraud or misuse of funds). In both programing and operations, high level risks can be a result of innovation and present tremendous opportunity to drive change.

### 3.10 How to evaluate risks?

Below are few tools and considerations to help evaluate identified risks:

***Risk Mapping:*** All risks of a particular programme/unit or project can be mapped across the ERM risk matrix using the ERM Dashboard (see previous section). The Dashboard presents an aggregated snapshot of the risk across the scale from Low to High (risk significance level). The mapping should help identify priority risks.

***Risk Proximity***. Proximity reflects the fact that risks may materialize at different times in the future. Knowing the proximity of a risk (when the risk is likely to happen) helps to identify the urgency and timing of the response. Risks that may materialize in the short term may be more urgent so an understanding of risk proximity helps to prioritize risks.

***Risk Capacities/Tolerance:*** Relates to the organization's or team's readiness to bear the risks and accept the consequences should they occur. It involves having the right resources and controls in place to "tolerate" the given risk. Capacities to take on risks may vary from office to office and even within an office. Internal Issues related to staffing and human resources, skills and expertise, financial resources as well as external issues related to context, security, stakeholders etc, need to be considered. The risk capacities and tolerance will vary depending on the particular risk and office. Note that UNDP corporate and regional risk management expertise can be drawn on as well to support risk capacities across the organization.

***Risk Appetite:*** Risk Appetite expresses the maximum amount and type of risk that UNDP is willing to accept in order to achieve its mandate and strategic objectives [NOTE: UNDP Risk Appetite Statement to be developed]. The Risk Appetite Statement (RAS) will not only provide a baseline for risk-tolerance for all UNDP country offices around the globe but also inform its stakeholders, donors, partners, and general public about the maximum level of risks the organization is willing to accept and how UNDP intends to address different risks to meet its plans, based on comprehensive evaluation possible threats and opportunities, to meet its plans.

# 4 Risk Treatment (and Escalation)

## 4.1 What is risk treatment and when is it required?

The purpose of risk treatment is to manage the risk's significance, by addressing either the likelihood or impact or both. For each risk one or more risk treatment measures must be identified.

## 4.2 How to identify risk treatment measures?

When a risk poses a threat to organizational objectives, the 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** (accepting the risk level).

When a risk presents an opportunity, the 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 treatment measures should be determined through a consultative process and informed by the risk analysis, particularly for High level risks. Relevant expertise should also be consulted to advise on appropriate risk treatment measures. While in some cases, best management practices can be applied, in other situations innovative risk management measures will need to be identified.

## 4.3 Who is accountable for risk treatment?

All risks must have a designated **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, i.e. an activity agreed within the team to modify the risk. The Risk Owner and Treatment Owner may or may not be the same individual. Ownership is assigned based on the accountability for managing the risk, noting that many people may need to be involved.

The Risk Owner and Treatment Owners are recorded in the **Risk Register**, which includes treatment activities, deadlines for their implementation.

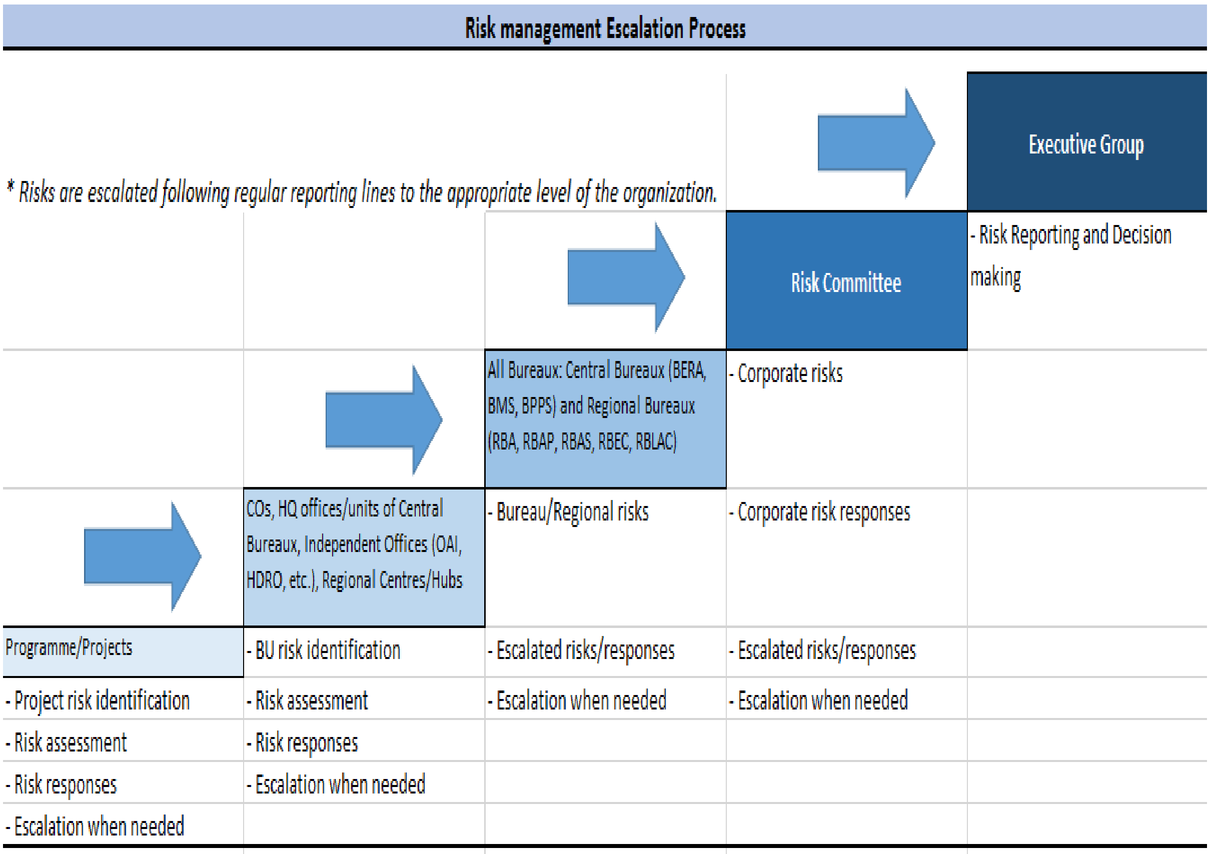
## 4.4 When and how to escalate risk?

Not all risks can be managed at the level where they are identified. 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.

To escalate a risk, the Risk Owner must provide complete information about the risk 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 and ultimately to the corporate level.




# 5 Risk Monitoring and Review

## 5.1 What is the purpose of risk monitoring and review?

The overall purpose of the risk review and regular monitoring is to ensure continued risk identification and analysis and effective risk treatment. This involves continuing to scan the changing internal and external context, reflect on how risk levels may be changing, emerging risks, and progress and relevance of risk treatment measures. Regular risk monitoring and review is an essential component of proactive ***adaptive management and course corrections***.

## 5.2 How to review and monitor risks?

Risk review and monitoring involves ongoing risk identification and analysis. Field visits and further risk assessments may be required. Real-time monitoring of opportunities and threats should be considered in rapidly changing contexts to provide an early-warning mechanism, enable proactive response and capitalize on available opportunities. Stakeholder engagement in risk monitoring can also be an effective way to strengthen monitoring and review.

**Recommended: Strategic Risk Sessions**
It is recommended to consider organizing regular meetings to discuss ***Strategic/ high-level Risks*** within each project, programme/unit, Bureaux. The purpose is to identify, analyze, and prioritize the risks. These meetings should involve programme/project

management team, thematic experts, procurement, HR, security, ICT, M&E, and other operations staff as relevant. When necessary and relevant the national counterparts and stakeholders could be engaged in these discussions as well.

At the corporate level, Strategic and escalated risks are identified and disused at the Risk Committee which is chaired by the Associate Administrator.

### 5.3 When to review and monitor risks?

Risk monitoring and review is an on-going process involving stakeholder engagement, data collection and analysis, and horizon scanning to inform adaptive decision-making and adjustments to overall risk management strategy.

## 6 Risk Recording and Reporting

### 6.1 What is the purpose of risk recording and reporting?

The purpose of risk recording and reporting is to ensure that all relevant stakeholders have a shared understanding and ownership of risks identified and risk management activities in due time. Risk reporting is an instrument for decision-making, transparency and compliance.

### 6.2 How to record and report on risks?

UNDP uses the Risk Register as the primary mechanism for recording risks at all levels. The **Corporate Planning System (CPS)Risk Register** is used to record Integrated Work Plans of programme/unit level with the associated risks and is also the basis for reporting of corporate risks to the EG and Risk Committee (see IWP Risk Register guidance). The **Project Risk Register**, based in Atlas, is used to record project level risks. For additional guidance see the Project Risk Register – Deliverable Description and Offline Template.

Risk reporting takes place at all levels: through the annual report to the EG and Risk Committee, the ROAR, and Project reporting. The format of project risk reporting might vary from project to project.

Ad-hoc reporting may also be needed, particularly in emergency contexts, if there is a need to report on risks to inform decision-making at a particular point in time, or based on requests from senior management, donors or stakeholders. An updated Risk Register provides the basis for ad-hoc and on-demand risk reporting.

Either as stand-alone or as part of the project or programme regular reporting, risk reporting will typically include the following:

- ✓ Risk summary/mapping
- ✓ Top risks, owners, and status of treatment actions
- ✓ Changes since last review

- ✓ Conclusions and recommendations (including lessons learned)
- ✓ Appendix: Complete risk register

### 6.3 When to record and report on risks?

The minimum risk reporting requirements prescribed in the ERM Policy are below:

- ***At the project level*** the project Risk Register is used for monitoring as often as needed, but no less than once a year.
- ***At the programme/unit*** an annual report through the ROAR and semi-annual report through IWP Risk Register.
- ***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.

Note that this minimum frequency is for compliance purposes but more regular risk recording based on the ongoing monitoring and review, should be conducted. The frequency will vary depending on context and risks and should be decided at the programme/unit and project levels.

## 7 Risk Communication and Consultation

### 7.1 What is the purpose of risk communication and consultation?

The purpose is twofold. *First*, is to ensure that relevant stakeholders are around the table when considering/identifying risks and risk management measures. The range of stakeholders varies depending on context and might include a variety of internal stakeholders (GPN experts, finance, HR, Security, etc.) as well as external partners from UN system, national partners, experts, donors, etc. *Second*, is to highlight the criticality of risk communication to inform your stakeholders about the risks identified, how they are managed, and therefore, to manage expectations on how to share responsibilities and accountabilities around various risks and their management.

### 7.2 Who to include in a risk consultation?

Inclusiveness is essential for effective risk management. As a starting point, key stakeholders are those directly affected by the risk. This includes internal teams and experts who have a role in managing these risks, donors whose funds are at stake, government and other partners, beneficiaries and affected people. It is critical to include all relevant stakeholders into risk identification, assessment, treatment, monitoring, reporting and review. Meaningful stakeholder engagement in the process enhances the completeness of your risk profile, the buy-in of risk response measures across your key stakeholders, early warning of emerging risks, and the success of your risk management efforts at large. It also builds stakeholder confidence in UNDP and ownership of the process and results.

## 7.3 When to convene risk consultations?

Risk consultations should occur on a regular basis. Strategic Risk Sessions, or other mechanisms to facilitate dialogue on risk, can also be convened to inform particular management decisions. Entry points to convene such discussions include:

***Develop UN Cooperation Framework/CPD:*** at this phase the focus of risk management is twofold: (a) on the risks in the country context towards the strategic development priorities of the country itself, and (b) on the organizational commitments and institutional capacities of UNDP to address those risks, which become for UNDP opportunities to invest for development results.

***Appraise and Approve:*** at this phase the focus of risk management should be on the risks UNDP country office might have vis-à-vis the defined strategy on how to support the national counterparts through Cooperation Framework/CPD.

***Annual Planning:*** at this stage the focus of risk management should be on emerging risks and changes in the existing risks to ensure there are necessary provisions for adequate risk response measures in the planning and necessary corrections in the course of actions.

***Monitoring and Oversight:*** at this stage the focus of risk management is to guarantee necessary assurance on the resources invested and results to expect.

***Reporting:*** at this stage the focus of risk management is to provide necessary information about risks and risk management efforts within the organization. EACH project and programme report MUST reflect on risk management.

***Programme Transition:*** at this stage the focus of risk management is to ensure there is complete overview of the risks that will be transiting with the project. This stage is of utmost importance for sustainability and impact of development results.

# Annex 1: UNDP 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<br>1.2. Gender<br>1.3. Biodiversity and use of natural resources<br>1.4. Climate change and disaster<br>1.5. Community health and safety<br>1.6. Labour conditions/standards<br>1.7. Cultural heritage<br>1.8. Rights of Indigenous Peoples<br>1.9. Displacement and resettlement<br>1.10. Pollution and resource efficiency<br>1.11. Stakeholder engagement<br>1.12. Sexual exploitation and abuse | 2.1. Cost recovery<br>2.2. Value for money<br>2.3. Corruption and fraud<br>2.4. Fluctuation in credit rate, market, currency<br>2.5. Delivery | 3.1. Alignment with national priorities<br>3.2. Responsiveness to lessons learned and evaluations<br>3.3. Leadership & management<br>3.4. Flexibility and opportunity management<br>3.5. Synergy potential (linking with other initiatives as relevant)<br>3.6. Reporting and communication<br>3.7. Partnership<br>3.8. Capacity development of national partners<br>3.9. Engagement of national partners in decision-making<br>3.10. Transition and exit strategy<br>3.11. Occupational safety, health and well-being | 4.1. Governance<br>4.2. Monitoring<br>4.3. Independence and quality of evaluation<br>4.4. Knowledge management<br>4.5. Grievances<br>4.6. Due diligence of private sector partners<br>4.7. Human Resources<br>4.8. Budget availability and cash flow<br>4.9. Internal control<br>4.10. Procurement<br>4.11. Innovating, piloting, experimenting, | 5.1. Government commitment<br>5.2. Political will<br>5.3. Political instability<br>5.4. Change/ turnover in government | 6.1. Changes in the regulatory framework within the country of operation<br>6.2. Changes in the international regulatory framework affecting the whole organization<br>6.3. Deviation from UNDP internal rules and regulations | 7.1. Theory of change<br>7.2. Alignment with UNDP Strategic priorities<br>7.3. Capacities of the partners<br>7.4. Roles and responsibilities among partners<br>7.5. Code of conduct and ethics<br>7.6. Public opinion and media<br>7.7. Synergy with UN / Delivery as One | 8.1 Armed Conflict<br>8.2 Terrorism<br>8.3 Crime<br>8.4 Civil Unrest<br>8.5 Natural Hazards<br>8.6 Manmade Hazards |

## Annex 2: Application of ERM Processes according to organizational levels

Application of ERM Processes according to organizational levels

| | IDENTIFY | | | EVALUATE | | | MONITOR | |
|---|---|---|---|---|---|---|---|---|
| | | ***Risk Assessment*** | | | | | | |
| *ERM Processes that apply across all levels of UNDP* | **Establishing the context** | **Risk identification** *(What and where are the risks?)* | **Risk analysis** *(What is known about the risks?)* | **Risk evaluation** *(How important are the risks identified?)* | **Risk reporting** *(What and how the risk should be reported?)* | **Risk treatment** *(What should be done about the risks identified?)* | **Monitoring & Review** | **Communications & consultation** |
| **Programme/Projects** | Programme and/or Project Document, Annual Work Plan (AWP) | Identify major risks for the programme/project objectives in the Programme/ Project Document and AWP. | Analyze likelihood and the consequences of the risks to identify those that might affect the achievement of the objectives of programme/ project. | Evaluate the risk levels of all analyzed risks at the project to determine which risks need treatment and their priority, in order to meet the objectives of the project AWP. | Quarterly monitoring & reporting on programme/ project risks; Report on progress and/or failure and results to the Project Board. | Identify one or more treatment options (terminate, mitigate, transfer or tolerate) and implement the most effective one/s. Escalate the risks that can't be adequately managed at the project level to the CO Sr. management. | Monitor effectiveness of RM processes at the project level; Update Risk Log on quarterly basis. | Keep the project Board and other stakeholders/partners informed on RM processes at the project and updated them regularly. |
| **Country Offices and HQ Units** | UN Development Assistance Framework (UNDAF); Country Programme Document (CPD); IWP of the CO and the HQ Unit | Identify major risks for the overall objectives in the CPD and the respective IWP of the CO and the Unit. | Analyze likelihood and the consequences of the risks identified at all projects, the CO and the Unit by applying the criteria model. | Evaluate the risk levels of all analyzed risks at projects, the CO and the HQ Units to determine which risks need treatment and their priority, in order to meet the objectives of the respective IWP. | Report the CO and HQ Units major risks info/data in their IWP and annual reporting (ROAR), e.g. risk level, treatment status. | Implement treatment options (terminate, mitigate, transfer or tolerate). Respond to the escalated risks. Escalate the risks that can't be adequately addressed at the CO and HQ Units to higher levels. | Oversight of RM processes and monitor their effectiveness in all projects, the CO and the HQ Units; Update Risk register on quarterly basis. | Keep the Programme Board, other stakeholders/partners of the CO and the HQ Unit informed on RM processes and updated them regularly. |
| **Central Bureaux, Regional Bureaux and Independent Offices (OAI, HDRO, etc.)** | Regional Programme Document; Bureau IWP; Office IWP | Identify major risks for the overall objectives across COs in the region, Central Bureaux and the Office level, and the respective IWPs. | Review all of the analyzed risks and identify trends and pattern in risks across COs in the region, Central Bureaux and the Offices. | Evaluate all of the analyzed risks across the COs in the region, Central Bureax and the Offices to define the risk level that the Bureau & Office is willing to accept in order to meet the IWP | Report the Bureaux and the Offices' major risks info/data in their IWP and annual reporting (ROAR). | Respond to the COs & Units' escalated risks; Escalate the risks that cannot be adequately addressed by Central/Regional Bureaux, and the Offices to the ERM Committee. | Oversight of RM processes and monitor their effectiveness in the COs across the region, Central & Regional Bureaux and the Offices; Update Risk register on quarterly basis. | Communicate & consult with revelant parties of the Bureau and the Office at all stages of RM processes and update them at regular/ planned intervals. |
| **UNDP Corporate** | UNDP Strategic Plan (SP); Annual Business Plan (ABP) | Identify major risks (both threats & opportunities) at corporate level affecting UNDP. | Review and analyze the overall UNDP risk profile and identify strategic risks and issues across the organization. | Strategic assessment of all the prioritized risks at corporate level and define the risk level that UNDP is willing to accept in order to meet its objectives in the SP. | Analyze and report the overall risk profile of UNDP; Prepare a quarterly and an annual risk reports to the EG, based on a strategic analysis of UNDP's overall risk landscape. | Escalate the risks from HQ units & all Bureaux for ERM Risk Committe consideration to make decisions on escalated corporate risks (prioritize them and specific actions to be taken). | Document the decisions taken by the risk committe in the Corporate Risk Log, and monitor and update it regularly. | The Risk Committee reports to the EG on quarterly basis. Prepares an annual UNDP risk report for considertaion of the EG through the Risk Committee. |

Risk Assesment