OPERATIONAL INSTRUCTION REF.OI.RCG.2025.01

RISK MANAGEMENT

Headquarters, Copenhagen

07 Apr 2025

1. Authority

1.1 This Operational Instruction (OI) is promulgated by the Director, Risk and Compliance Group under OD.FG.2018.03: Risk Management.

2. Purpose

2.1 The purpose of this OI is to provide instructions with a view to operationalising UNOPS enterprise risk management framework as set out in OD.FG.2018.03 Risk Management, in particular with respect to the governance, infrastructure and process pertaining to risk management in UNOPS.

2.2 It also provides instructions on how this process shall be executed, thereby supporting relevant UNOPS personnel in fulfilling their roles and responsibilities

3. Effective Date

3.1 This OI shall become effective on 07 May 2025

4. Consequential changes

4.1 This OI supersedes and replaces OI.FG.2022.02: Risk Management, to reflect the creation of the Portfolio Oversight Committee (POC) and the discontinuation of the Engagement Acceptance Committee (EAC - no longer operational as of 7 May 2025). It also incorporates minor updates, including revised unit names, simplified risk documentation requirements, and other related adjustments - pending a more comprehensive revision.

[signature redacted]

Ynvgil Foss

Director, Risk and Compliance Group

Table of Contents

- 1. Introduction (see page 2)
- 2. Roles and Responsibilities (see page 2)
- 3. UNOPS Risk Tolerance (see page 3)
- 4. Key Levels for Risk Management (see page 4)
- 5. UNOPS Standard Risk Management Process (see page 6)
- 6. Risk management tools and taxonomies (see page 8)

1. Introduction

1.1. This OI provides instructions to operationalise and implement the enterprise risk management framework set out in the OD.FG.2018.03: Risk Management, with the aim of fostering consistent and effective risk management across the organization.

1.3. The OI sets out roles and responsibilities, as well as the key risk management practices, tools and taxonomies, to be used for risk management activities.

2. Roles and Responsibilities

2.1. The roles and responsibilities for risk management in UNOPS are defined in OD.FG.2018.03: Risk Management and further elaborated below:

- The **Executive Office (EO)** shall be accountable to the Executive Board for overall risk management in UNOPS.
- The UNOPS **Portfolio Oversight Committee (POC)** shall support the Executive Director (ED) in ensuring High-Stake Engagements are managed at [1] (see page 10) the right level and in a way that protects the Organization, while maximizing UNOPS impact.
- The **UNOPS Management Team (MT)** shall act as UNOPS risk committee and shall regularly review UNOPS corporate risk landscape.
- The **heads of functional and geographical entities** (e.g. heads of groups, as well as heads of offices for region, country, multi-country, project, centre, city, or cluster) shall be accountable for the effectiveness of risk management conducted within their respective entity, including for escalating key risks to senior leadership, as necessary.
- **Management at functional and geographical entity level** (e.g. those with managerial responsibilities in a group, an office for region, country, multi-country, project, centre, city, or cluster) shall be responsible for coordinating the risk management process within their respective area of responsibility. This shall include promoting and enabling an open risk management culture as well as monitoring risk exposure at lower management levels. While risk management should be seen as a shared responsibility across all management, entities may decide to allocate the responsibility to specific roles within the entity.
- **Management at the engagement level** (e.g. project/programme manager) shall be responsible for coordinating the risk management process within their respective area of responsibility. This

shall include promoting and enabling an open risk management culture as well as monitoring effectiveness of risk management at lower management levels.

- The **Engagement Authority** (e.g. assigned DoA holders for engagement acceptance and for engagement assurance) shall be accountable for the risk [2] (see page 10) management within his/her engagement portfolio, and shall have overall authority for the engagement acceptance, assurance and decision making on key risks.
- The **Project Board Executive**, once appointed, shall have delegated authority for risk management at the project level and shall ensure effective project risk management, including responding to and escalating risks, as necessary.
- **Policy units** shall be responsible for monitoring risk exposure within their area of responsibility to ensure alignment with UNOPS legislative framework and best practices.
- **Engagement reviewers** shall be responsible for reviewing engagements, providing advice on operational risk management at all stages of the project lifespan to support and improve alignment with UNOPS legislative framework and best practices. This includes engagement acceptance reviews and advice during implementation and closure.
- A **risk owner** is an individual who is appointed the responsibility to manage and monitor a specific risk, including identifying and ensuring the effective implementation of risk responses.
- A **risk actionee** is an individual assigned to carry out a risk response action or actions to respond to a particular risk or set of risks, on behalf of the risk owner.
- The **Risk Unit - Risk and Compliance Group (RCG)** shall be custodian for UNOPS ERM framework and for the approach to corporate risk management. This also includes providing technical risk management expertise and training.
- **The Infrastructure and Project Management Group (IPMG)** shall be responsible for UNOPS Portfolio Oversight Committee (POC) secretariat - with the support of the RCG . IPMG is also responsible for quarterly assurance (QA) [3] (see page 10)reporting and for establishing tools/guidance for operational risk management.
- **Stakeholders** and **team members** shall be consulted and/or informed during all stages of the risk management process.
- **All UNOPS personnel** shall abide by the enterprise risk management framework and actively engage in risk management activities, when relevant.

3. UNOPS Risk Tolerance

3.1. UNOPS shall specify risk tolerance levels for certain identified types of risks, i.e. thresholds or specific criteria that, when exceeded, require risk response(s) and/or escalation. Risk tolerance levels shall thus define the boundaries for when certain risks have to be treated or escalated.

3.2. Management of specific entities within UNOPS may define additional escalation processes tailored to their specific context.

4. Key Levels for Risk Management

4.1. UNOPS ERM comprises three key levels for risk management:

- Corporate (UNOPS as a global entity)
- Organizational (geographical entities)[4] (see page 10)
- Operational (projects, programmes and portfolios - together “engagements”)

4.2. Risks shall be escalated from one level to the next, when the risks are estimated to have an impact on objectives also on a higher level.

4.3. The mandatory risk management activities and guidance for the flow of risk information across the three levels are described below.

4.4. The level of risk management effort shall be proportional to the complexity and uncertainty surrounding the entity’s objectives and key activities - across all risk management levels. Greater complexity demands a more robust and adaptive approach. Professional judgment shall be applied to align the effort to the specific context and needs.

Operational Risk Management

4.5. Operational risk management relates to managing operational risks to facilitate successful delivery of UNOPS engagements.

4.6. Risk management shall be carried out throughout all stages of the engagement ; from opportunity to implementation and closure stages.

4.7. The mandatory risk management activities for this level are set out below.

4.8. Some engagements may have a substantial impact on beneficiaries and may also expose the Organization to very high residual risks - including reputational, financial, legal, compliance and other major consequences (e.g. mandate mis-alignment, social and environmental safeguards, fraud and corruption, etc.). These shall be classified as High-Stake Engagements and are in the purview of the POC.

4.9. Engagements may be identified as High-Stake Engagements by the Engagement Authorities and/or the Review & Policy Units at any stage of the engagement lifespan, from early opportunities and acceptance to implementation, closure and post-handover liabilities.

4.10. Engagements with high-risk exposure that require policy exception(s) and/or other corporate de-risking measures are reviewed in consultation with relevant policy units. Such cases do not require escalation to the POC unless the engagement can be considered high-stake.

4.11. UNOPS shall provide guidance to personnel involved in developing and managing [5] (see page 10) engagements and partnerships on the organization's expectations for escalating engagement decisions through UNOPS line of authority. This shall be read in conjunction with other applicable escalation guidance, including - among others - the engagement acceptance high risk list.

Risk management during engagement development

4.12. Risks shall be managed and documented (as per the Project Management Manual) for all new opportunities and engagements. Risk management shall begin at an early stage, so that it informs engagement acceptance decisions and resulting agreement. Where possible, risk responses shall be

determined and/or implemented before accepting the engagement and entering into the resulting agreement.

4.13. Risk management is led by those with managerial responsibilities in an entity. It shall be seen as a collaborative exercise engaging relevant stakeholders, including subject matter experts and partners.

Responsible	Accountable	Consulted	Informed
Management at the entity level (e.g. those with managerial responsibilities for opportunity and engagement acceptance)	Engagement authority (relevant DoA holder)	Reviewers Policy units POC Secretariat (for High-Stake Engagements)	Team members Relevant stakeholders

Risk management during implementation and closure

4.14. Key risks and issues are continuously managed and documented throughout the implementation and closure stages.

4.15. Depending on the size and complexity of the engagement, management at the engagement level may decide to create project-level risk registers as alternative or in addition to the engagement-level risk register.

Responsible	Accountable	Consulted	Informed
Management at the project and engagement level (e.g. Project/ programme manager)	Project level: Project board executive Engagement level: Engagement authority (e.g. Head of programme, country/ Multi-Country Office director)	Reviewers Policy units POC Secretariat (for High-Stakes Engagements)	Team members Relevant stakeholders

Organizational Risk Management

4.16. Organizational risk management relates to managing risks at geographical entity level (e.g. offices of region, country, multi-country, project centre, city or cluster), such as risks to the reputation and financial viability of an office or the successful achievement of the entity's objectives.

4.17. The mandatory risk management activities for this level are set out below. *Organizational risk assessment*

4.18. Entities shall regularly manage key risks within their area of responsibility, including any given risks originating from the operational level, if these are estimated to potentially have an impact on entities' objectives. Key risks and issues should be continuously managed and documented as part of applicable assurance processes (quarterly assurance for country/multi-country offices) and following any significant changes to the entity's internal or external context.

4.19. When a risk materializes, thereby turning into an issue, this shall be recorded in the entity's issue register and managed accordingly.

4.20. It shall be possible to escalate risks for review and/or decision making of higher level of management, when considered appropriate or when standard criteria are met.

4.21. Entities shall monitor and review their entity-level risk exposure during applicable assurance processes.

Responsible	Accountable	Consulted	Informed
For risk management: Management at entity level (e.g. those with managerial responsibilities in the entity, incl. head of entity)[6] (see page 10) For country/multi country assurance: Country/ multi country director (or HoPs with required DoA)	For risk management: Head of entity (e.g. head of region, country/multi country or group) For country/multi country assurance: Regional director	Reviewers Policy units POC Secretariat (for High-Stakes Engagements)	Team members Relevant stakeholders

Corporate Risk Management

4.22. Corporate risk management relates to managing risks to UNOPS as a global entity, such as risks to the reputation and financial viability of UNOPS.

Periodic risk review

4.23. UNOPS shall establish and maintain an overview of its corporate risk landscape, embedded into key decision making context and reviewed periodically by the Management Team as part of relevant business review processes.

Responsible	Accountable	Consulted	Informed
MT	EO	Policy units RCG - Risk Unit	Relevant stakeholders

5. UNOPS Standard Risk Management Process

5.1. UNOPS has defined a standard risk management process to guide personnel and management in structuring their risk management activities, whether at operational or organizational level.

5.2. The process is inspired by internationally recognized standards and tailored to UNOPS context.

5.3. The process is an iterative process with six key steps that are illustrated and described below.



Establish the Context

5.4. When planning a risk assessment, the first step shall be to define its scope and focus. This includes considering the internal and external context, such as considering linkages to objectives and stakeholder expectations, as well as consulting subject matter experts and reviewing relevant lessons learned.

Risk Assessment

5.5. The risk assessment includes identifying relevant risks, analysing the sources to the risks and their potential consequences, as well as evaluating the potential impact, probability of occurrence and proximity of the risk.

5.6. The assessment will include classifying risks according to UNOPS standard risk categories, as set out in section 6 below.

5.7. An important component of the assessment is to identify risk owners for all identified risks to ensure that these are continuously managed and monitored.

5.8. The risk assessment shall be documented and recorded so that it can be regularly reviewed and maintained.

Risk Response

5.9. The risk owner shall ensure that response plans are defined and implemented. This includes escalating risks in line with guidelines. Response actions should be categorized in accordance with UNOPS standard risk response categories.

5.10. Risk actionee(s) shall be assigned to all risk responses, so that it is clear who is responsible to take action.

Monitoring and Review

5.11. Monitoring and review of risks shall take place during all steps of risk management to assure and improve the quality and effectiveness of the process. This shall include monitoring the effectiveness of implemented responses and updating risk assessments to reflect changes in the internal and/or external context.

Communication and Consultation

5.12. Communication and consultation with stakeholders (internal and external) shall take place throughout all steps of risk management to increase adequacy and reliability of risk information.

5.13. Communication and consultation also helps promote risk-awareness, and UNOPS shall foster an open risk culture to support continuous improvement and learning across the organization, while also taking into account information sensitivity and privacy.

Reporting

5.14. The risk management process and its outcomes shall be documented and reported using UNOPS risk management tools to support portfolio data aggregation and to assist management and oversight bodies in meeting their responsibilities.

6. Risk management tools and taxonomies

6.1. The standard tools and taxonomies to be applied are set out below and are further specified in guidance documents under this OI.

Standard Risk Categories

6.2. UNOPS risk categories provide a structure to help identify and evaluate risks, while also allowing risks to be grouped to provide overview and enable prioritization.

6.3. The risk categories shall be aligned with the categories in UNOPS balanced scorecard so that risks are clearly linked to UNOPS objectives and performance management. The categories and guidance for these shall be described in PQMS.

Standard Risk Evaluation Scale

6.4. UNOPS risk evaluation scale defines risk levels that illustrate the magnitude of a risk. The risk level is defined by combining the estimated impact (the consequences of the risk materialising) and likelihood (the probability that the risk will materialise). There are four risk levels on the scale:

- 1 = Low
- 2 = Low to Medium
- 3 = Medium to High
- 4 = High

6.5. The criteria to distinguish between these levels shall be defined in PQMS.

6.6. Risk level shall be assessed as the current level of risk after considering any given existing controls or already implemented risk responses. This allows the organization to focus on which additional controls/responses are needed to ensure that the risk is within acceptable tolerance levels.

6.7. The evaluation shall also consider the risk proximity, which is an estimate of when the risk could materialise, as expressed in time intervals applied in UNOPS risk management information system.

Standard Risk Response Categories

6.8. Risk management responses are classified in accordance with the below taxonomy:

- *Avoid:* eliminate the probability and/or impact of a threat
- *Exploit:* seizing an opportunity in order to increase its probability and/or impact *Reduce:* diminish the probability and/or impact of a threat
- *Enhance:* increase the probability and/or impact of an opportunity *Transfer:* a third party takes on the responsibility for the impact of a threat *Share:* distribute the risk among several parties
- *Accept:* retain and monitor a threat that is considered tolerable
- *Contingency plans:* accept the risk for now and prepare a plan in case the situation changes (i.e. plan B)

Risk Management Information System

6.9. UNOPS shall implement a risk management information system that is aligned with UNOPS standard risk taxonomies to support effective risk management at organizational and operational levels.

6.10. The system shall serve as repository and action plans for risks at organizational and operational levels.

Footnotes

[1] As defined under par. 4.8 of this Operational Instruction

[2] The POC Chair is accountable for decision(s) taken on high stake engagements and partnerships. Once accepted, the accountability for engagement assurance follows the assigned DoAs.

[3] Risk and Compliance Group supports the Secretariat by: co-developing guidance on what constitutes High-Stake Engagements, maintaining relevant Submission Form(s) and decision preparation template(s), supporting the escalation process co-facilitating decision preparation on engagements escalated to the Committee

[4] At this time, the requirements set out in sections 4 to 6 of this OI do not apply to functional entities.

[5] Ref. Management of Engagement and Partnership Escalation - Guidance Note 2025

[6] While risk management should be seen as a shared responsibility across all management, entities may decide to allocate the responsibility to specific roles within the entity