Headquarters, Copenhagen
28 September 2018

OPERATIONAL INSTRUCTION REF. OI.FG.2018.06

RISK MANAGEMENT

1. Authority:

1.1. This Operational Instruction (OI) is promulgated by the Chief Financial Officer under OD.FG.2018.03 Risk Management, on the basis of a delegation of authority from the Executive Director (ED).

2. Purpose:

2.1. The purpose of this OI to provide instructions with a view to operationalising UNOPS enterprise risk management framework 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 immediately.

3.2. Requirements in OI section 4.11-4.21 and section 6 will only become mandatory after full roll-out of UNOPS Enterprise Portfolio and Project Management solution (oneUNOPS Projects).

[signature redacted]

Marianne de la Touche, O.i.C., Finance Groupe

UNOPS

OPERATIONAL INSTRUCTION REF. OI.FG.2018.06

RISK MANAGEMENT

Table of Contents

1. Introduction

1.1. This OI provides instructions to operationalise and implement the risk management principles set out in the OD with the aim of fostering consistent and effective risk management across the organization.

1.2. The section 'UNOPS Enterprise Risk Management' explains how risk management is implemented in practice throughout UNOPS' established processes at all levels. The section 'UNOPS standard risk management process' is a generic methodology that can be followed to carry out risk management at any given level.

1.3. The OI also sets out roles and responsibilities, as well as introduces the risk management tools and taxonomies to be applied for risk management activities.

2. Roles and Responsibilities

2.1. The roles and responsibilities for risk management in UNOPS are defined in the OD on risk management and further elaborated below:

- The **Executive Office (EO)** shall be accountable to the Executive Board for overall risk management in UNOPS.
- The expanded **Corporate Operations Group (COG)** shall act as UNOPS risk committee, which shall regularly review UNOPS corporate risks.
- The **heads of geographical and functional entities** (e.g. head of offices for region, country, multi country, project, group, 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 geographical and functional entity level** (e.g. those with managerial responsibilities in an office for region, country, multi country, project, group, 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 project and 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 risk exposure 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 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 owners** shall be responsible for monitoring risk exposure within their area of responsibility to ensure alignment with UNOPS legislative framework and best practices.
- **Reviewers** (e.g. IPAS and other assigned subject matter experts) shall be responsible for 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 Finance Group (FG)** shall be responsible for corporate risk management and custodian of UNOPS ERM framework. This shall include providing technical risk management expertise and training.
- **The Infrastructure and Project Management Group (IPMG)** shall be responsible for UNOPS engagement acceptance committee (EAC) secretariat and quarterly assurance (QA) reporting. IPMG is also responsible 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.

** The EAC is accountable for acceptance of high risk engagements. Once accepted, the accountability for engagement assurance follows the assigned DoAs.*

3. UNOPS risk tolerance

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

3.2. Management of specific entities within UNOPS (such as geographical/function entities or engagement/projects) may define additional tolerances tailored to their specific context.

4. UNOPS Enterprise Risk Management (ERM)

4.1. UNOPS ERM provides a framework for how risk information shall flow across the organization to ensure that risks are addressed at the appropriate level of management.

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

- Corporate (UNOPS as a global entity)
- Organizational (geographical and functional entities)
- Operational (engagements, projects, and portfolios)

4.3. These three risk management levels can be depicted as hierarchical, where risks are escalated from one level to the next, when the risks are estimated to have an impact on objectives also on a higher level.

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

Operational risk management

4.5. Operational risk management relates to managing risks at project and programme level to facilitate successful delivery of UNOPS engagements.

4.6. Risk management shall be carried out throughout all stages of the project lifespan; from opportunity to closure.

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

Risk management during engagement development

4.8. A risk assessment shall be conducted and documented in a risk register (as per the Project Management Manual) for all new opportunities and engagements. It shall be initiated at an early stage, so that relevant risks can inform and be accounted for in the engagement acceptance process and resulting agreement. Where possible, risk responses shall be decided and/or implemented before accepting the engagement and entering into the resulting agreement.

4.9. Risk assessments are led by those with managerial responsibilities in an entity. The assessments shall be seen as a collaborative exercise engaging all relevant stakeholders, including subject matter experts and partners.

4.10. Engagements with high-risk exposure that may have potential organization-wide consequences shall be escalated via the regional office to the engagement acceptance committee (EAC) for review, in accordance with the OI on acceptance of engagement agreements.

Responsible	Accountable	Consulted	Informed

Management at the entity level (e.g. those with managerial responsibilities for opportunity and engagement acceptance)	Engagement authority (Regional director or EAC)	Reviewers Policy owners FG (ERM) IPMG (EAC/QA)	Team members Relevant stakeholders

Risk management during implementation and closure

4.11. The engagement risk register created during the engagement development shall be continuously reassessed and managed throughout the implementation and closure stages.

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

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

4.14. The engagement risk register shall be reviewed during established assurance processes.

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/hub director)	Reviewers Policy owners FG (ERM) IPMG (EAC/QA)	Team members Relevant stakeholders

Organizational risk management

4.15. Organizational risk management relates to managing risks at geographical or functional entity level (e.g. offices of region, country, multi country, project, group, 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.

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

Organizational risk assessment

4.17. Entities shall regularly undertake risk assessments to 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. Such assessments should, as a minimum, be conducted on an annual basis as an integral part of setting management work plans. Assessments should be reviewed as part of

applicable assurance processes (quarterly assurance for country/multi countries offices) and following any significant changes to the entity's internal or external context.

4.18. Entities shall document their risk assessment in the entity's risk register, and continuously manage identified risks. This includes ensuring that relevant internal controls to manage the risks are implemented and effective.

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 (as defined in 'standard criteria for response, review and escalation') are met. Escalation triggers the transfer of risk ownership to the next management level (e.g. from country to region, or from region to EO).

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*) 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 owners FG (ERM) IPMG (EAC/QA)	Team members Relevant stakeholders

** 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*

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.

Quarterly risk review

4.23. UNOPS shall establish and maintain an overview of its corporate risks, which shall be reviewed periodically by the COG to enable risk-informed decisions.

Responsible	Accountable	Consulted	Informed
COG	EO	Policy owners FG (ERM) IPMG (EAC/QA)	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.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

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 facilitate decision making and to support management and oversight bodies in meeting their responsibilities.

6. Risk management tools and taxonomies

6.1. Risk management activities at operational and organizational levels shall be carried out using UNOPS standard risk management tools and applying standard risk taxonomies, as this allows risks to be interlinked and evaluated across entities and risk management levels.

6.2. The key taxonomies to be applied are set out below and will be further specified in guidance documents under this OI.

Standard risk categories

6.3. Risk management activities shall be done applying the defined risk categories. These provide a structure to help identify and evaluate risks, while also allowing risks to be grouped to provide overview and enable prioritization.

6.4. 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

6.5. Risk assessments shall apply UNOPS risk evaluation scale below to define 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

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

6.7. 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.

6.8. 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

6.9. Risk management responses shall be categorised in accordance with UNOPS standard risk responses, as listed below:

- *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)

Standard criteria for response, review and escalation

6.10. Standard criteria to direct identification of risk responses, review frequency, and escalation requirements are established in UNOPS risk management information system tool. These criteria are defined by specific triggers, such as the risk evaluation level and EAC criteria. Entities may tailor certain criteria in the risk management information system tool to reflect their specific context.

Risk management information system

6.11. UNOPS shall implement a risk management information system that is aligned with UNOPS standard risk taxonomies to support effective risk management at all levels.

6.12. The system shall serve as repository and action plans for risks at all levels, enabling monitoring and escalation across levels.