



Enterprise Risk Management and Internal Control

A guide for the implementation of an UNEP-wide Framework Implementation

July 2021

Produced by Clara Elisabeth Stickers

United Nations Avenue, Gigiri

PO Box 30552 – 00100, Nairobi, Kenya

Tel: +254207623568 | clara.stickers@un.org

www.unep.org

I	Table of Contents	2
1.	EXECUTIVE SUMMARY	3
2.	BACKGROUND	6
3.	PURPOSE	6
4.	DEFINITION	7
5.	ENTERPRISE RISK MANAGEMENT PROCESS AT UNEP	9
	5.1. <i>Establishing the Context</i>	11
	5.2. <i>Consideration of Risks and Objectives</i>	14
	5.3. <i>Event Identification and Risk Assessment</i>	19
	5.4. <i>Risk Response and Internal Control Activities</i>	30
	5.5. <i>Information and Communication</i>	35
	5.6. <i>Monitoring and Assurance</i>	41
6.	RISK GOVERNANCE, ROLES AND RESPONSIBILITIES	42
	6.1. <i>ERM Leadership at the Secretariat</i>	43
	6.2. <i>ERM leadership at UNEP</i>	47
	6.3. <i>ERM drivers at UNEP</i>	48
	6.4. <i>Risk owners at UNEP</i>	50
	6.5. <i>ERM Oversight and accountability at UNEP</i>	51
7.	FINAL PROVISIONS	52
	Appendix 1: <i>Glossary of Terms and Definitions</i>	53
	Appendix 2: <i>United Nations Secretariat-wide Risk Universe</i>	55
	Appendix 3: <i>Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control</i>	56
	Appendix 4: <i>UNEP Risk Management Committee Terms of Reference</i>	58
	Appendix 5: <i>Phased Implementation and Implementation Roadmap</i>	60
8.	ANNEXES	62

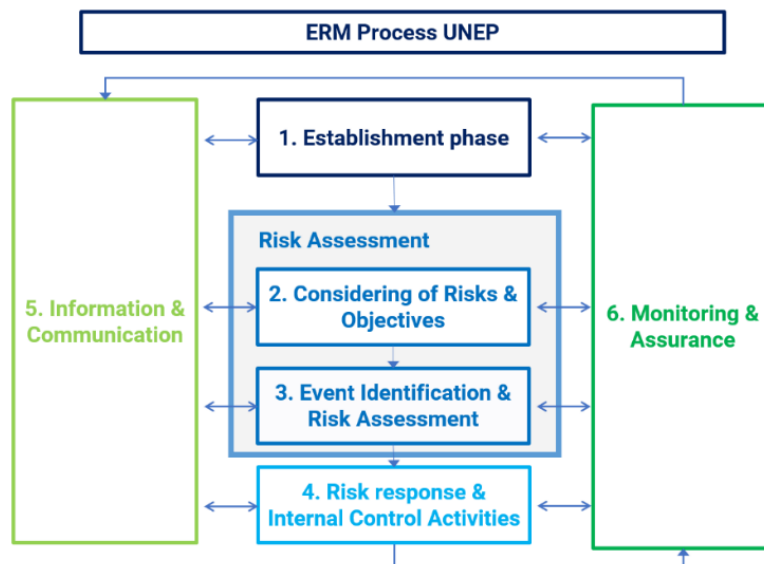
1. Executive Summary

These guidelines serve to outline the process that will facilitate the implementation of an effective risk management framework in UNEP - in compliance with the UN-Secretariat Enterprise Risk Management and Internal Control (ERM/IC) Policy and Methodology as adopted by the Secretary-General in May 2011.

Enterprise Risk Management (ERM) facilitates effective strategic decision-making as it provides management with the necessary tools to fully understand the root causes of risk and design proper response strategies. By prioritizing the response on critical risk areas, it progressively contributes to informing the strategic planning and resource allocation process, enabling senior managers to make sound, properly informed decisions. The prevailing line of thought is that risks are not purely hazards to be avoided: risks per se also provide opportunities. Within this context, ERM has emerged as a structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties an organization faces as it pursues its objectives.

The Enterprise Risks Management Process at UNEP

In the initial stages of implementation UNEP will follow the recommendations emanating from the UN Secretariat's Policy (last updated August 2020) and appropriate steps arising from best practice studies. An approach based on 'top-ten' risk areas, inventory of current risk-response activities and deriving prioritization of treatment plans for the evidenced gaps is the most advisable strategy. The total estimated time from start of the ERM/IC programme to launch of the Risk Treatment Plan is 28 weeks, consisting the following steps:



Q2- 2021 will be spent on the analysis of the risk areas defined by various auditing reports, budgets, and other policy and organizational documentation. The UNEP SMT will collectively discuss, validate and propose changes to the outcomes as appropriate, and endorse the timeline, implementation strategies and guidelines.

Q3- 2021 will be consumed with establishment of the Risk Management Committee, and the execution of validation workshops that bring together technical leads and senior staff members to define measurement of Impact, Likelihood and Level of Internal Control effectiveness. The designated Risk committee will be tasked with the review of the validation workshops, the risk prioritisation, the finalisation of UNEP’s updated Risk Register, and the assigning Risk owners.

Q4- 2021 will be used to validate the first stage of the ERM implementation with UNEP’s risk register and dashboards created, scoring criterion for the measurement of Impact, Likelihood and Level of Internal Control effectiveness reviewed and endorsed bet the SMT, and response and treatment plans drafted for top risks identified as priority.

Phase	Implementation	Q3 2021	Q4 2021	Q1 2022	Q2 2022	Q3 2022	Q4 2022
1 – Establishment	Draft and endorsement of ERM framework	■					
	ERM Sensitisation period	■	■				
2&3 – Risk Assessment	Identification and assessment of corporate level risks	■				■	
	Validation of priority risks	■	■				
	Statement Internal Control (SIC)			■		■	
4 – Risk Response & Internal Control Activities	Design of Treatment and Response (TR)		■	■			
	Implementation of TR-plans			■	■	■	■
6 – Monitoring & Assurance	Monitoring and feedback loop				■	■	■
5 – Information & Communication	ERM Training	■					
	Periodic Risk Reporting		■	■	■	■	■

Q1 and Q2- 2022 is set for the monitoring of the Risk Treatment Plans and preparation for the feedback loop. ERM is a continuous improvement process and the framework will evolve accordingly. Each year the risk universe is updated expanding its coverage of UNEP's operations both in scope and depth: a selection of new, or additional risks of second priority level, may be taken to the successive treatment plan stage.

The ERM framework will be implemented in phases with some activities taking place in parallel sequences in order to optimize the full benefits of the exercise. The end of the implantation cycle – after the first feedback loop - is target at mid-2022. Full implantation of the Framework is set for December 2022 – [Appendix 5](#).

Risk Governance at UNEP

In accordance with the Secretariat's Enterprise Risk Management policy, UNEP's Executive Director is responsible for the effective implementation of risk management. UNEP's Executive Director shall constitute a *UNEP Risk Management Committee*, the Senior Management Team (SMT) to align and coordinate activities related to risk management matters.

The Committee shall serve as a forum to build consensus on key strategic areas by validating and prioritizing risks; identifying trends and emerging risks; and reviewing and recommending measures to proactively manage risks.

Reporting to the Executive Director and the Senior Management Team (SMT), the Committee will perform the following functions:

- i. Validate and prioritize risks identified across the entity and determine the risks to be reflected in the risk register; and escalate any issues to the Senior Management Team (SMT);
- ii. Ensure the alignment of the risk management framework with the Secretariat-wide Policy and Methodology;
- iii. Review the final Risk Register prior to submission for approval to the Executive Director;
- iv. Perform ongoing reviews and updates of the Risk Register and identify emerging risks, and determine the risks to be added or downgraded from the risk register;
- v. Submit the consolidated plan of risk treatment measures to the Executive Director and escalate any issues to the Senior Management Team (SMT);
- vi. Deal with any other relevant risk management and internal control matters.

UNEP recognizes that ERM is not a 'one size fits all' approach. The key is to determine the degree of maturity that is right for the Organization and the specific needs of senior management to tailor - while maintaining full compliance to the Secretary-General's policy - an ERM/IC programme that is appropriate for UNEP.

2. Background

Enterprise Risk Management (ERM) facilitates effective strategic decision making in a modern organization. It fosters healthy dialogue at the most senior managerial level on the critical matters the United Nations is facing in an environment of growing complexity and uncertainty. It supports enhanced accountability and contributes to the implementation of a best practice governance framework, through the transparent prioritization and clear ownership of objectives, risks, and managerial responses.

The implementation of the United Nations Environment Programme Risk Management is adapted from the Secretariat-wide ERM and Internal Control framework and is guided by the following documents:

- i. **Policy document** outlining the purpose, governance mechanisms and principles that guide the adoption of ERM in the Organization. It was formally approved by the Management Committee in May 2011 and presented to the General Assembly in March 2012 ([Annex 1](#)).
- ii. **ERM Guide for Managers**, describing the *Methodology* and concrete steps for implementing ERM across the Secretariat ([Annex 2](#)).

3. Purpose

The main purpose of this Guide is to lay out clearly each step of ERM implementation for the practitioner to follow along. The Guide is divided into three sections: the first part is devoted to definitions of risk and ERM. The second part introduces the ERM framework which provides functional structure for implementing the ERM process. And the last part focuses on risk governance that includes the way in which ERM roles and responsibilities are divided in the organizational structure.

A consistent ERM framework with a UNEP-wide scope and a robust, yet practical governance structure are essential to ensure the alignment in the understanding of objectives and related risks at different levels of the Organization, and with Governing Bodies – as it promotes transparency and facilitates open discussions on strategic issues, enhancing stakeholders' confidence.

The UNEP-wide ERM process provides management with the necessary tools to fully understand the root causes of a risk, make results across UNEP comparable and design proper response strategies. Prioritizing the response on critical risk areas, it progressively contributes to informing the strategic planning and resource allocation process, *enabling senior managers to make sound, properly informed decisions*.

“One of the greatest contributions of risk managers – arguably the single greatest – is just carrying a torch around and providing transparency” An ERM Officer

4. Definition

Consistent with the best international standards risk is defined as an “an effect of uncertainty on objectives”. Effect is generally thought of as a deviation from expected. It can be positive, negative or both, and address, create or result in opportunities and threats.

ERM, on the other hand, is a structured process. It is defined as:

“The process of coordinated activities designed to direct and control an organization with regard to risk, the effect of uncertainty on objectives.¹ It is effected by governing bodies, management and other personnel, and applied in strategy-setting throughout the Organization”.

Accordingly, an effective *system of internal control* is encompassed within and is an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualisation and tool for management.



ERM addresses the strategic, governance and financial risks associated with the execution of the mandates and objectives as defined by the Charter of the United Nations, as well as the operational risks inherent in the daily operations that support the achievement of those mandates.

Implementation of the ERM with a balanced focus among all risk categories enhances the governance and management practices of the Organization, as outlined below:

- i. **Focus on Objectives** – Increased effectiveness in the achievement of the defined objectives and mandates through a consistent identification, assessment, and management of risks in UNEP.
- ii. **Internal Controls** – Embedded risk and internal control management activities, enabling risk management to become an integral part of the processes and operations of the entire Organization, and determining the type of risk mitigation or corrective measures necessary to manage the identified risks.
- iii. **Efficient Use of Resources** – Improved performance against objectives, contributing to reduced waste and fraud, better value for money, and a significantly more efficient use of available resources.

¹ “Risk management – Principles and Guidelines” – International Organization for Standardization, 2018.

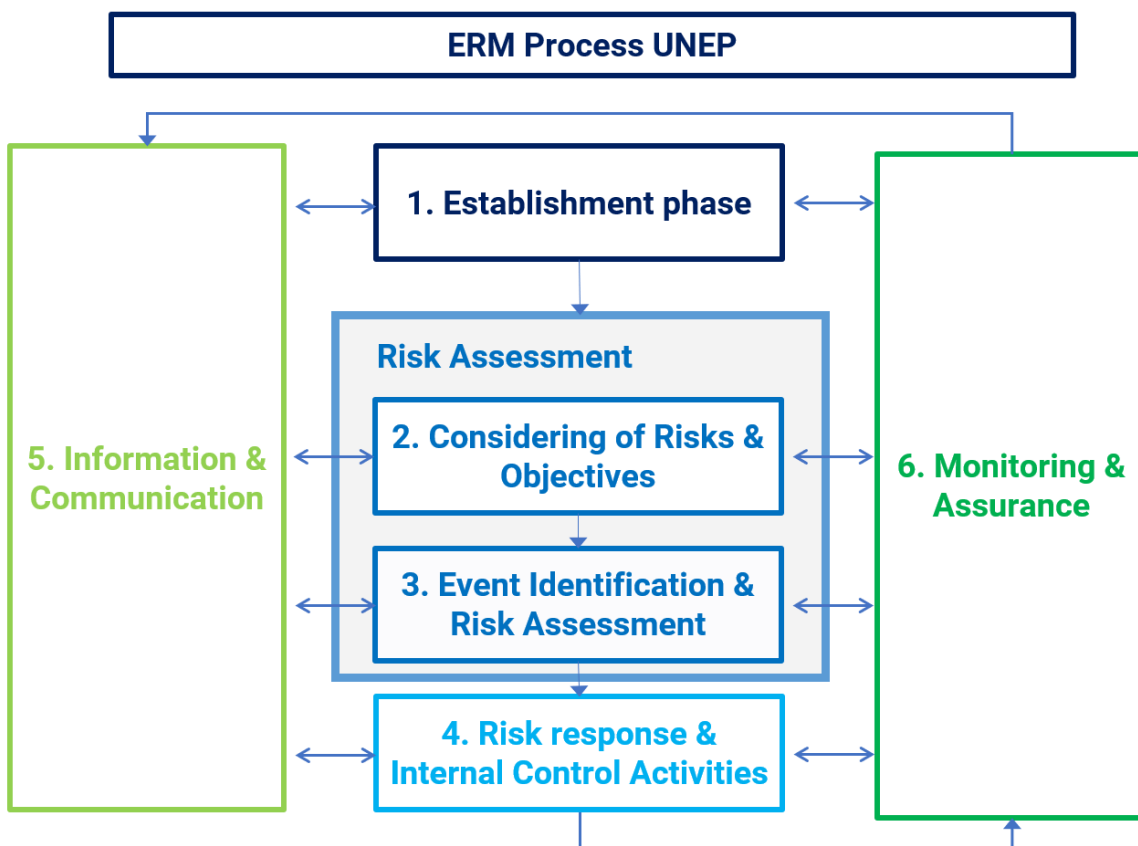
- iv. **Accountability** – Enhanced accountability and performance management through the definition of clear risk management roles and responsibilities.
- v. **Results Based Management** – Promotion of a risk driven culture through a more informed risk based decision-making capability, as the significance of risks and the effectiveness of designed controls are explicitly considered when evaluating programmes and relevant budget allocations, according to an effective results-based management approach.
- vi. **Transparency** – Improved transparency within the Organization and towards member states, as risks are clearly communicated internally and externally through periodic formal reporting by management to the Independent Audit Advisory Committee (IAAC) and the General Assembly.
- vii. **Assurance** – Improved assurance over internal controls through the formal recognition of management’s responsibility for effective controls, and the appropriate management of risks.
- viii. **Oversight** – The ability to enhance governance and oversight functions.
- ix. **Governance** – An increased capability of senior management and governing bodies to make informed decisions regarding *risk/reward trade-offs* related to existing and new programmes, through the adoption of a structured approach for the identification of opportunities to enhance the allocation of resources throughout the Organization and reduce related costs.

5. Enterprise Risk Management process at UNEP

ERM is a continuous, evolving and integrated process owned and executed by management. ERM is not a periodic validation exercise, it evolves over time in accordance with the pace and scope of the changes, and it integrates with other UN Entities with the objective of merging both risk and return information into strategic planning and decision making. The ultimate goal of this process is to make the ERM a part of the Organization’s culture.

The main components of the risk management process cycle are illustrated in Figure 1 below, and further described in this section of the document. This cycle steps operate within the functional ERM framework structure. The definition of all the relevant terms is included in [Appendix 1](#) of this document – **Glossary of Terms and Definitions**.

Figure 1- Enterprise Risk Management Process Cycle



In particular:

- i. **Establishing the Context** – Establishing the context encompasses the definition of the Organization’s overall risk management approach, as outlined by the Policy articulating the purpose, governance mechanisms, and principles that guide the adoption of the framework.
- ii. **Consideration of Risks and Objectives** – Risks are mapped and aligned to objectives, mandates and strategic initiatives in the Organization. Specific measurement criteria for risk evaluation are also defined.
- iii. **Event Identification and Risk Assessment** – Risks are assessed in the context of the objectives, mandates and strategic plans through interviews, risk questionnaires, workshops with relevant management and staff, and other sources. The analysis of trends in recommendations from oversight bodies could also provide important indications. Identified risks are then measured and scored according to the perceived impact, likelihood and level of managerial and internal control effectiveness.
- iv. **Risk Response** – Risks are prioritised based on the overall ratings for each risk in terms of risk exposure and then, through the consideration of the level of risk mitigation and internal control effectiveness, in terms of *residual risk*. Appropriate risk treatments are determined based on the overall risk prioritisation and implemented according to defined timelines and responsibilities. An effective system of internal control is an integral part of enterprise risk management.
- v. **Information and Communication** – Ongoing reporting on results of risk assessments, including risk treatment plans and actions, is established. Appropriate communication and training programs are developed across the Organization to nurture the development of a sound risk aware culture and build adequate capacity and critical skills.
- vi. **Monitoring and Assurance** – Ongoing monitoring of risks and internal controls are implemented.

A detailed description of the specific steps to be followed in the implementation of an effective enterprise risk management and internal control framework is provided below.

5.1. Establishing the Context

In order to provide direction to the process of implementation of the ERM framework, UNEP has adopted an overall Enterprise Risk Management and Internal Control Policy, articulating the principles that guide the adoption of the framework.

The ERM and internal control framework at UNEP is guided by the following **core principles**:

- i. **Embedding** – Risk management must be explicitly embedded in existing processes. Appropriate flexibility needs to be applied in the execution of strategies and allocation of relevant resources through the proper consideration of the risks that could affect the achievement of the objectives applicable to UNEP, and the overall Secretariat.
- ii. **Consistency** – UNEP shall adopt, as part of its decision-making process, a consistent method for the identification, assessment, mitigation, monitoring and communication of risks associated with any of its processes and functions, in an effort to efficiently and effectively achieve its objectives.
- iii. **Integration** – The ERM and internal control framework must be fully integrated with the major operational processes, such as strategic planning, operational and financial management, and performance measurement and management within UNEP and the MEAs.
- iv. **Results-based management** – Risk management shall be integrated with the adoption of an effective results-based management approach. ERM complements results-based management by enabling to effectively achieve set objectives with a clear, shared understanding of the internal and external uncertainties that may impact activities. High priority risks and the effectiveness of related controls shall also be fully considered in the evaluation of programmes and relevant budget allocations.
- v. **Agility** – As UNEP is in a constant state of motion, the enterprise risk management framework must enable agile processes to react, respond to and address changes to the Organization. Program and policy changes, new corporate opportunities, technology shifts, reorganized business processes and other factors will constantly barrage the Organization, and the risk and compliance implications must be managed in a manner that permits UNEP to consume, adjust to and manage these changes.
- vi. **Transparency** – The concept of transparency should permeate the enterprise risk management framework. Transparency means delivering the right information to the right stakeholders within timeframes necessary for the purposes of enabling effective governance, informing Organizational analysis and providing (senior) management with information that can be leveraged. This transparency extends to both internal and external stakeholders and

includes overall visibility into the structure of the framework and the results documented and managed within the exercise (such as the alignment of strategies and objectives, risk management processes, risk priority, risk responses, internal controls and compliance with internal and external obligations). It is through the transparency of the enterprise risk management framework that positive assurance of its effectiveness is demonstrated.

The effective implementation of the framework within UNEP relies as well on:

- i. **Management Ownership** – Risk owners and management across UNEP– the Senior Management Team, Directors and Project Managers - must have a sound understanding of the risks impacting their operations, and the level of flexibility provided to appropriately determine the available and appropriate course of action to manage those risks, increasing accountability.
- ii. **Inclusion (of MEA's)** – UNEP's Global structure needs to be reflected throughout the enterprise risk management framework in such a way that all parts of the entity – with special attention to the Multilateral Environmental Agreements – are fully integrated as part of the risk assessment, risk response and treatment, risk monitoring, risk oversight and communication, and internal control processes.
- iii. **Risk Aware Culture** – A risk-focused and results-oriented culture shall be nurtured, moving the Organization from the current predominantly risk adverse culture, where the focus is merely on risk avoidance, to a risk aware culture, where decisions are driven by a systematic assessment of risks and rewards. The dissemination of information and best practices regarding risk and internal control management principles shall be supported across the Organization, developing appropriate communication and training programs.
- iv. **Communication** – Adequate information shall be provided to senior management, the Management Committee, the Secretary-General and the General Assembly. The governing body, with the advice of the ERM Committee on Administrative and Budgetary Questions and the Independent Audit bodies, will be then in a position to effectively fulfil its responsibilities of provision of governance and oversight, and to take decisions on the acceptance of proposed modifications or enhancements of the internal control system.
- v. **Client Orientation** – Easy to use, automated processes should be designed to drive efficiencies by taking copied spreadsheets, email, file sharing and manual processes out of the equation as much as possible, and by employing tools and workflows to automate processes. Automation should ensure that the right people are engaged to contribute information and make decisions, at the right time, with the right information, based on corporate requirements and best practices – easing the process and making the ERM exercise as accessible as possible to all actors involved.

Commitments

The strong support and commitment of the Executive Office and the Senior Management Team are essential for the establishment of effective risk and internal control management processes. A sustainable framework is therefore based on:

- i. **Support** – The endorsement and consistent support from the Executive Office and the Senior Management Team, confirmed by visible actions, is critical for the successful implementation of the framework
- ii. **Accountability** – The adoption of an effective framework relies on the full ownership and accountability of Directors and Risk Owners throughout the Organization for risk management and internal control activities.
- iii. **Resources** – Risk and internal control management shall be supported by Administration Unit in the Corporate Services Division which will be the Secretariat and will provide expert guidance in the implementation of Enterprise Risk Management.
- iv. **Collaboration** – UNEP needs to reinforce collaboration across the Organization on matters of risk and compliance management without regard to organizational boundaries – in attempt to break silos. Collaboration introduces diversity in problem-solving through information sharing, analytics and tracking the right metrics to make the right decisions at the right time.

5.2. Consideration of Risks and Objectives

"If one does not know to which port one is sailing, no wind is favorable"
Seneca

5.2. a UNEP Tailored Risk Catalogue

The initial stages of the risk assessment process require the alignment and mapping of risks to the underlying strategies, plans and objectives, based on UNEP's **Risk Universe** drafted in 2014. The updated Risk Universe, attached to this Guide as [Annex 3](#), presents a high-level description of all the risks relevant to the Organization, and shall be tailored, as required, to reflect the profile of the organizational unit under consideration. Based primarily on its mandates and objectives, as well as its strategies and operations, each division/office shall develop its own risk catalogue as a sub-set of the UNEP Risk Universe, so that eventually, all risks identified within the Organization shall be traced back to the corporate-level Risk Universe. It might be worthwhile to note that although the risk universe is comprehensive, it might not be exhaustive, as new and emerging risks could arise.

Through a common taxonomy of risks and an agreed set of definitions, the Organization adopts a common risk language, and becomes able to collect and appraise risk information on multiple levels across the entire Organization and evaluate it in a consistent and integrated manner. Through this process, UNEP will also be able to understand the impact of various alternate response strategies on an organization-wide basis, as well as to assess the overall effectiveness of existing internal controls and measures of risk mitigation.

The tailored **Risk Catalogue** at division and office level should be based on the experience of the division or office. In this perspective, process flow analyses, incident reports, the results of previous risk assessments, and a detailed *analysis of trends and common areas in past recommendations of oversight bodies* could provide extremely valuable indications. The consideration of anticipated future activities could also provide very useful indications.

In order to be able to accurately reflect the operations of each level, the definition of the entity-level risk catalogue based on the UNEP-wide risk taxonomy should allow some degree of flexibility. Where needed, entity-specific risks could be created under the relevant risk categories, or existing risks could be divided in specific sub risks.

Example

Customization of the UNEP risk catalogue

The UNEP-wide risk catalogue could be tailored to the specific risks identified at division or office level through the creation of sub-risk areas, e.g.

4. Operations: 4.2 Human Resources, sub-dividing the risks as follows:

- | | |
|---|---------------------|
| 4.2.2 – Recruiting, Hiring, and Retention | 4.2.2.1. Recruiting |
| | 4.2.2.2. Hiring |
| | 4.2.2.3. Retention |

The Risk Universe of the Secretariat identifies and defines a catalogue of 133 risks, categorized into seven major risk areas: (1) Strategic, (2) Governance, (3) Managerial, (4) Operational, (5) Financial, (6) Compliance, and (7) Fraud and Corruption risks. The definition of each risk is provided in the Risk Catalogue that complements this Guide.

Enterprise Risk Management process at UNEP

Figure 2: United Nations Secretariat Risk Universe (Appendix 2)

1 STRATEGIC	2 GOVERNANCE	3 MANAGERIAL	4 OPERATIONS	5 FINANCIAL	7 FRAUD and CORRUPTION
1.1 Planning	2.1 Governance	3.1 General Management	4.1 Support Services	5.1 Funding and Investments	7.1 Fraud Control Environment
1.1.1 Vision and Mandate	2.1.1 Tone at the Top	3.1.1 Mgmt of Org. Transformation	4.1.1 Translation and Interpretation	5.1.1 Financial Contributions	7.1.1 Organizational Culture & Envirmnt
1.1.2 Strategic Planning	2.1.2 Control Environment/ Risk Mgmt	3.1.2 Leadership and Management	4.1.2 Procurement	5.1.2 Extra-budgetary Funding	7.1.2 ICT Governance & Cyber Security
1.1.3 Budgeting	2.1.3 Organizational Structure	3.1.3 Staff/Management Relations	4.1.3 Supplier Management	5.1.3 Trust Fund Management	7.1.3 Umoja System Control Envirmnt
1.1.4 Budget Allocation	2.1.4 Transparency		4.1.4 Asset and Inventory Management	5.1.4 Donor Fund Mgmt & Reporting	
1.1.5 Prog Performance Measurement	2.1.5 Accountability	3.2 Programme Management	4.1.5 Facilities and Real Estate Mgmt	5.1.5 Cash Management	7.2 Programme Delivery
1.1.6 Planning Execution & Integration	2.1.6 Empowerment	3.2.1 Advocacy	4.1.6 Capital Master Planning	5.1.6 Investments	7.2.1 Political Influence on Prog Reprtn
1.1.7 HR Strategy and Planning		3.2.2 Outreach Activities	4.1.7 Business Continuity	5.1.7 Financial Markets	7.2.2 Implementing Partners
1.1.8 Organizational Synchronization	2.2 Ethical behaviour	3.2.3 Economic and Social Development	4.1.8 Commercial Activities	5.1.8 Insurance	7.2.3 Contingent-Owned Equipment
1.1.9 Outsourcing	2.2.1 Ethics	3.2.4 Research, Analysis and Advisory			7.2.4 Theft: Fuel, Rations, Inventory
1.1.10 Org. Transf.n & Mgmt Reform	2.2.2 Sexual Exploitation and Abuse	3.2.5 Human Rights	4.2 Human Resources	5.2 Accounting and Reporting	7.3 Human Resources
	2.2.3 Professional Conduct	3.2.6 Humanitarian Assistance	4.2.1 Resource Allocation & Availability	5.2.1 Financial Mgmt and Reporting	7.3.1 Educational/Professional Creds
1.2 Principal Organs, Partners	2.2.4 Sexual Harasment	3.2.7 Disarmament	4.2.2 Recruiting, Hiring and Retention	5.2.2 General Accounting	7.3.2 Recruitment
1.2.1 GA and Member States		3.2.8 Combatting Terrorism	4.2.3 Training and Development	5.2.3 Financial Controls	7.3.3 Payroll: Attendance, Travel, Leave
1.2.2 Partners and Donors	2.3 Communications and PR	3.2.9 Crime Prevention/Drug Control	4.2.4 Performance Management	5.2.4 Liability Management	7.3.4 Benefits and Allowances
1.2.3 Inter-Agency Coordination	2.3.1 Media Relations and PI	3.2.10 Policy Development	4.2.5 Succession Planning & Promotion	5.2.5 Staff Tax Reimbursements	7.3.5 Medical Insurance
	2.3.2 Crisis Communications	3.2.11 Inter-agency Programme Coop.	4.2.6 Mobility		7.3.6 Gifts, Entertainment, Travel
1.3 Internal & External Factors	2.3.3 Internet, Soc Media, Radio, TV	3.2.12 Conference Management	4.2.7 Compensation and Benefits	6 COMPLIANCE	7.3.7 Conflicts of Interest
1.3.1 Political Climate - External	2.3.4 Technology Communication	3.3 Mission activities	4.2.8 Discipline and Conduct	6.1 Legal	7.4 Central Services
1.3.2 Political Climate - Internal		3.3.1 Peacekeeping/SPM Mandates	4.2.9 Healthcare Management	6.1.1 Contract	7.4.1 Procurement
1.3.3 Economic Factors - Commodity		3.3.2 Electoral Support	4.2.10 Occupational Safety and Health	6.1.2 Intellectual Property	7.4.2 False Statements & Laissez Passer
1.3.4 Unique Events (i.e. Pandemic)		3.3.3 Rule of Law	4.2.11 Security	6.1.3 Anti-Corruption	
1.3.5 Climate Change		3.3.4 Mission Planning	4.3 Intellectual Property	6.1.4 International Law	
		3.3.5 Mission Start-up	4.3.1 Knowledge Management	6.1.5 Privacy	
1.4 Reputation		3.3.6 Mission Liquidation	4.3.2 Information and Document Mgmt	6.2 Regulatory	
1.4.1 Public Perception & Reputation		3.3.7 Logistics	4.4 Information Resources & IT	6.2.1 Internal Policies and Resolutions	
1.4.2 Crisis & Contingency Mgmt		3.3.8 Air, Land and Sea Operations	4.4.1 IT Strategy	6.2.2 UN Labour Relations	
		3.3.9 Engineering	4.4.2 IT Security and Access	6.2.3 Host country regulations	
		3.3.10 Communications	4.4.3 IT Availability and Continuity		
		3.3.11 Mission staffing	4.4.4 IT Integrity		
		3.3.12 Mission Creep	4.4.5 IT Infrastructure		
		3.4 International tribunals	4.5 Environmental Sustainability		
		3.4.1 Investigations and Prosecution	4.5.1 Environmental Management		
		3.4.2 Trials and Appeals			
		3.4.3 Legal Aid			
		3.4.4 Court Mgmt & Legal Support			
		3.4.5 Witness Protection			
		3.4.6 Detention Unit Management			
		3.4.7 Completion Strategy			
		3.4.8 Residual Capacity and Activities			

5. 2. b Scoring Criteria for the measurement of risks

Following the definition of the objectives and scope of the risk assessment, the scoring criteria for the measurement of risks shall be determined. According to best practice, risks will be measured in terms of:

- i. **Impact** – The result or effect of an event.
- ii. **Likelihood** – The possibility that a given event will occur.
- iii. **Level of Internal Control / Management Effectiveness** – The perceived effectiveness of the internal controls, processes and activities in place to manage or mitigate a risk. In this context, internal controls are defined as the processes, effected by an entity's governing body, management and other personnel, designed to provide reasonable assurance regarding the achievement of its set objectives.

The Organization has defined the scoring criteria for the measurement of impact, likelihood and level of control effectiveness in mitigating risk at the Secretariat and entity level, as described in [Appendix 3](#) of this Guide. Where applicable, the common criteria shall be *tailored* to UNEP and its risk profile and operations. For example, the absolute terms of the potential financial impact should be adjusted to the size of UNEP's budget, and the description of the organizational scope should be tailored to UNEP's governance and structure.

Figure 3 – Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control / Management Effectiveness (Appendix 3)

Impact

Score	Rating	Description of Impact					Financial impact (measured in terms of budget)	Recovery Required action to recover	
		Safety and security	Duration	Organizational and operational scope	Reputational impact	Impact on operations			
5	Critical	Loss of life (staff, partners, general population)	Potentially irrecoverable impact	Organization-wide inability to continue normal business operations across the Organization.	Reports in key international media for more than one week	Inability to perform mission or operations for more than one month	>5 per cent >\$500 million	Requires significant attention and intervention from General Assembly and Member States	
4	Significant	Loss of life due to accidents/non-hostile activities	Recoverable in the long term (i.e., 24-36 months)	Two (2) or more departments/offices or locations: significant, ongoing interruptions to business operations within 2 or more departments/offices or locations	Comments in international media/forum	Disruption in operations for one week or longer	3-5 per cent \$300 million-\$500 million	Requires attention from senior management	
3	High	Injury to United Nations staff, partners and general population	Recoverable in the short term (i.e., 12-24 months)	One (1) or more departments/offices or locations: moderate impact within one or more departments/offices or locations	Several external comments within a country	Disruption in operations for less than one week	<2-3 per cent \$200 million-\$300 million	Requires intervention from middle management	
2	Moderate	Loss of infrastructure, equipment or other assets	Temporary (i.e., less than 12 months)	One (1) department/office or location: limited impact within department/office or location	Isolated external comments within a country	Moderate disruption to operations	<1-2 per cent \$100 million-\$200 million	Issues delegated to junior management and staff to resolve	
1	Low	Damage to infrastructure, equipment or other assets	Not applicable or limited impact					<1 per cent <\$100 million	Not applicable or limited impact

Likelihood

Score	Rating	Certainty	Frequency
5	Expected	>90 per cent	At least yearly and/or multiple occurrences within the year
4	Highly likely	<90 per cent	Approximately every 1-3 years
3	Likely	<60 per cent	Approximately every 3-7 years
2	Unlikely	<30 per cent	Approximately every 7-10 years
1	Rare	<10 per cent	Every 10 years and beyond or rarely

Internal Control / Management Effectiveness

Score	Rating	Description
5	Effective	Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks
4	Limited improvement needed	Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified
3	Significant improvement needed	Key controls and/or management activities in place, with significant opportunities for improvement identified
2	Ineffective	Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and are somewhat ineffective in efficiently mitigating risk or driving efficiency
1	Highly ineffective	Controls and/or management activities are non-existent or have major deficiencies and do not operate as intended. Controls and/or management activities as designed are highly ineffective in efficiently mitigating risk or driving efficiency

5.3. Event Identification and Risk Assessment

Starting with the UN Secretariat risk catalogue, potential risks at UNEP level shall be identified by collecting information from relevant management and staff members within the organizational unit that is conducting the risk assessment. The **time horizon** for the risk identification and assessment is targeted to be annual. A variety of techniques could be used for data collection, ranging from risk questionnaires and surveys, to individual interviews and workshops, or a combination of those.

5.3.a Programme-based approach

UNEP will deploy **a programme-based approach**, where there is a single overarching corporate risk register and risk management process, as well as derived risk registers for the decentralized units, such as the outposted, regional, or country offices, or MEA's.

Under a project-based approach, each individual project typically has its own risk register and risk management process. As a result, a single field operation or decentralized unit may have multiple risk registers and risk management processes that are not necessarily all at the same stage at the same time.

5.3.b Risk questionnaires and surveys

Whilst risk questionnaires and surveys could be useful to gather information from a wide number of participants in a relatively limited time, their contribution to an effective assessment process is deemed somewhat limited, as they may be perceived as a bureaucratic exercise failing to stimulate proper thinking and discussion on relevant risk areas. In addition, due to lower response rate of surveys, they may not serve as an authoritative data source and shall be complemented by in-person interviews. Taking into consideration the limited off-line access a **Sample Questionnaire and Sample Survey** which could help guide the risk assessment - if needed - can be found in [Annex 4](#) of this paper.

5.3.c Risk interviews

In light of the limitations surrounding surveys and questionnaires, **one-on-one interviews** with members of the senior management team appear to be a much more effective and powerful tool. They stimulate important conversations about risks, contributing to the progressive creation and strengthening of a risk aware culture at all levels.

The number of interviews depends on the size and governance structure of the office or division. They should include all the members of the senior management team (D level and above) and a sensible representation of field offices or areas and sections with specific focus or exposure to unique risks. As per the guidance of the Secretariat a number of interviews between 20 and 30 should be able to provide a comprehensive and balanced range of responses.

Linking risks to strategic objectives, they are an excellent vehicle to disseminate information related to risks and a unique source of meaningful discussions. They give the opportunity of confidentially expressing concerns to senior officers who not always might be comfortable in sharing sensitive information in a group setting. Senior officials could of course also choose to hold **small workshops** instead, inviting to attend a small group of their closest advisors, should they prefer so. Workshops are an excellent opportunity for sharing risk information, thanks to the enriched discussions they generate. One-on-one interviews usually can be effectively completed in about 45 minutes to an hour; small workshops could take slightly longer, in order to give all the participants, the opportunity to effectively contribute to the conversation. It would be ideal if the ERM team could be represented by two colleagues, if possible, one leading the conversation, the other taking detailed notes.

The interviews, which should be of course of *confidential nature*, are facilitated by UNEP's Risk Management focal point(s) and require quite a high level of tact and interviewing skills. Starting with the consideration of the relevant objectives for the entity for the period under consideration, and the potential risks to those objectives identified during the initial desk review, as well as taking into consideration the Secretariat risk catalogue, managers are invited to share their views on the most critical risk areas which in their opinion might impact the ability of the entity to achieve its mandates. Providing a visual representation of the preliminary risks (similar to the Risk Dashboard presented in Figure 4) might help in guiding the discussion.

Managers might start discussing their experience and areas of direct responsibility, and then expand their view to the entire operations of the entity. Personalities might be quite different. Every manager brings to the conversation their individual approach and perspective, and the difference in perspectives represents an important value to the risk assessment process. Some managers might limit to discussing the high level most strategic risks, without providing an opinion on risk ratings and relevant trends, other might have a much more analytical approach and describe in detail risk areas, related drivers and the effectiveness of designed controls and managerial responses. A **Sample Questionnaire and Sample Survey** which could help guide the risk assessment and discussion is provided in [Annex 4](#) of this paper.

It is of course essential that each contribution is properly interpreted by the ERM function and focal points as an important piece to create the mosaic that is the risk

register at the entity level. The interview should apply a Socratic approach, eliciting knowledge and understanding of risks through a semi-structured series of questions and answers, acquiring the confidence of the interviewee and at the same time gathering adequate information for the proper analysis of risks and controls.

5.3.d Outposted validators

The best practices “Paper Managing Risks in the Field and for Decentralized Organisations 2 Sep 2020”² in addition recommends using a corporate online risk assessment tool with a pre-defined (HQ) corporate risk register. This risk assessment is submitted online with justification for each of the risks to regional, MEA, or outposted offices for their review and validation. The outposted validators are staff familiar with the regional context, typically relevant desk officers. The outposted validators review and validate the country office assessment based on the data inputs and the justification provided. This also serves as the first line of quality review of individual risk assessments by the Headquarter. The outposted validators also consult relevant thematic focal points within the regional office for different thematic risk factors to take a considered view before rejecting/validating the risk assessment.

Outposted offices know the context of their region well and can therefore provide a much better informed and relevant review than the more distant HQ would be able to. As the agency also follows a regional focal point mechanism for other thematic areas, this approach is useful in consolidating other thematic inputs as well during the risk assessment stage. The involvement of the outposted offices can also help in planning and taking a regional risk perspective of the organization. The outposted office also acts as the first level of support for resolving the risk related issue and presents a bird’s eye view of the region in terms of top risk

5.3.e External Context

The external context is the environment in which UNEP operates and seeks to achieve its objectives and mandate. External risks are exposures that result from environmental conditions that the Organization commonly cannot influence, such as the political climate and economic conditions. Consideration should be given to the following inputs as they relate to the business operations, social, regulatory, legislative, cultural, competitive, financial, and political environment, including:

- i. Trends and factors related to geography, economy, climate, natural hazards, political, security, poverty level, corruption, criminality, etc.

² [Draft Paper Managing Risks in the Field and for Decentralized Organisations 2 Sep 2020](#)

- ii. Relationships with, perceptions and values of, external stakeholders such as partners and donors.

Various data sources and evidence can be drawn from external risk reports within the Secretariat – for example UNDP’s Crisis Risk Dashboard³, or global risk assessment such as the World Economic Forum’s Global Risk Report⁴ and the EURASIA group Top Risks⁵ and EURASIA Group Coronavirus edition Top Risks⁶ as part of the Enterprise Risk Management assessment the external context will be analysed, and ideas deriving from this assessment will be included in the risk report and subsequently disclosed to the SMT.

*“I myself know nothing, except just a little,
enough to extract an argument from another man who is wise and to receive it
fairly.” Socrates*

5. 3. f Risk assessment

Each of the identified risks shall be then evaluated by the ERM team according to the pre- defined risk and internal control rating criteria. As a first step, each risk will be scored in terms of the risk likelihood and impact, based on the information obtained through the interviews, workshops, surveys or process analyses. At this stage, we are considering the “largest credible risk”, as the **Risk Exposure** in the case of simultaneous failure of several controls established to mitigate the risk. From a methodological perspective, for the Secretariat the risk exposure can be determined by taking the square root of impact multiplied by likelihood (resulting therefore in a number between 0 and 5):

Risk exposure = Square Root (Impact x Likelihood)

Input to assess the effectiveness of internal controls or managerial processes in place to mitigate the risk should be then evaluated. The proper assessment of internal controls will of course depend on a thorough understanding of their intended purpose – i.e. how they intend to reduce the likelihood or impact of a defined risk, and their operational effectiveness. In practical terms, **Residual Risk** will be calculated as the difference between risk exposure on one side, and the level of internal control

³

https://public.tableau.com/profile/thiago.andrade3442#!/vizhome/UNDP_Crisis_Risk_Dashboard/UNDP_Crisis_Risk_Dashboard

⁴ <https://www.weforum.org/reports/the-global-risks-report-2020>

⁵ <https://www.eurasiagroup.net/issues/Top-Risks-2020> and [document](#).

⁶ <https://www.eurasiagroup.net/live-post/top-risks-2020-coronavirus-edition> and [document](#).

effectiveness on the other, (expressed therefore in a number potentially between -5 and 5):

$$\text{Residual risk} = \text{Risk exposure} - \text{Level of internal control}$$

To facilitate the calculation of the residual risk for each risk, the ERM function developed an easy to use calculator which is shared on its Community of Practice site², as well as, on the ERM page on I-seek and can also be found in [Annex 5](#) of this document.

According to best practice, residual risk is the risk remaining after management has taken action to alter the risk's likelihood or impact and shall therefore be the starting point for determining the appropriate treatment response. Based on the consideration of the resulting level of residual risk, and most importantly judgement on contributing factors and data gathered during the risk assessment process, risks shall be classified into three tiers.

Very High risks, categorised as *Tier 1 ("Red")* risks, are the most significant risks to which the entity is deemed to be exposed to, and will require an adequate level of attention. They shall be reported to the relevant Head of Office or Division, and the central ERM function, so that they could be consolidated with other risk areas emerging in different areas of the Organization, and accordingly reported to the Management Committee, and through the Secretary-General to the IAAC and the General Assembly.

High risks (*Tier 2 – "Orange"*) and **Medium risks** (*Tier 3 – "Yellow"*) will typically require specific remedial or monitoring measures under the responsibility of the specific Risk Owners and local Risk Management Focal Points, under the overall guidance of the relevant heads of entity.

If deemed appropriate by the relevant management, the register might as well include **Lower level risks** which could materialise quickly and have significant impact in a short span of time, and which should therefore be periodically monitored. Such risks could be as well classified according to their "speed of onset", or *velocity*. As an example, the risks related to the political volatility of a specific country, and/or the related security situation, could be reflected as *Lower ("Green")* risks in the Risk Register, as a tool for management to keep the evolving situation under close monitoring, even if the risks as presently assessed were not deemed to be among the most critical.

5.3.g Prioritization

In order to ensure a strategic and an effective approach, it is important that the assessment focuses on a relatively **small number** of risk areas with the largest potential to impact on UNEP. The vast majority of risks listed in the original risk taxonomy will probably be considered lower level risks, whilst based on the experience of the Organization it is reasonable to expect the risk assessment to consider and analyse in detail approximately the most important 10 to 20 risks. For example, the Secretariat-wide Risk Register has prioritized about 16 very high- risks.

UNEP's risk assessment from 2014 focussed on 4 **Very High** risks (HR Strategy and Reform, Organizational Transformation and UMOJA, Accountability and Empowerment, and Safety and Security) 2 **High risks** (Strategic Planning and Budgeting, and Trust Fund Management) and 6 **Medium** risks (Budget Allocation, Control Environment and Risk Management, Organizational Structure and Synchronization, Talent Management, ICT Strategy, Infrastructure and Security, Extra Budgetary Funding). For reference find the Risk Assessment in [Annex 3](#)

The **prioritization** process is crucial, as it should allow creating a short list of 5 to 10 high risk areas (the "top risks", or "tier 1 risks") which would require the immediate attention of senior management. Based on the UN experience, even merely listing the risks in order of *residual risk exposure*, from the highest to the lowest, would help to identify a potential gap or threshold above which risks might be considered most critical for the entity. The numerical values above which risks can be considered "**Very High**", "**High**" or "**Medium**" are shown in the risk calculator, and also depend on the particular risk profile and risk tolerance of the individual entity, and continue very much to rely on judgement based on the qualitative elements emerging from the risk assessment process.

² https://unitednations.sharepoint.com/sites/DMSPC-BTA_COMMS/SitePages/ERM-Resources.aspx

Example

Prioritization of Fraud and Corruption Risks

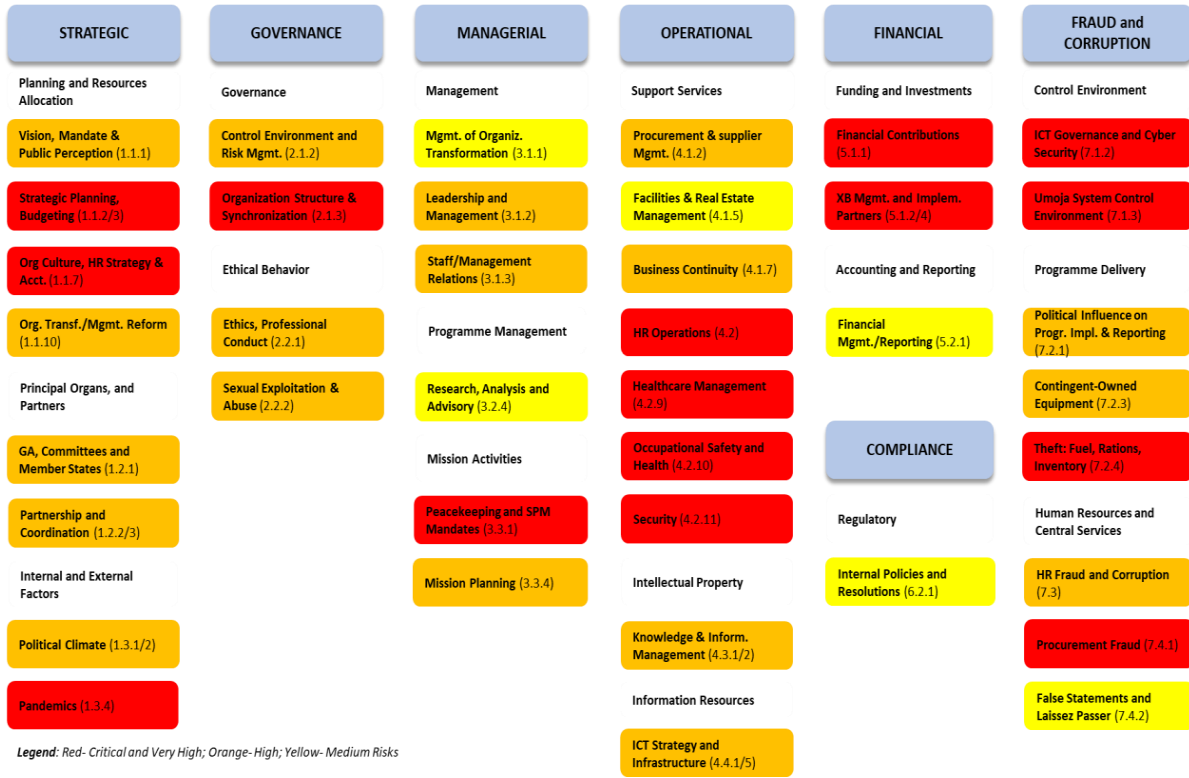
As part of a recent specific assessment of fraud and corruption risk areas within UNEP, the dedicated risk owners considered as "very high" all the risks with a residual risk exposure higher than 1, and "high" the ones between 0 and 1. Risks with a residual risk exposure lower than 0 were considered "medium".

As mentioned above, it is important to note that numerical values need to reflect the specific risk tolerance of the areas under review, and judgement should be applied considering the specific circumstances.

The entity risk register will not be an exhaustive list of all possible risks, which would be probably extremely long and unmanageable, but a profile of the most significant risks facing the entity, from a senior management strategic perspective. It is also important to note that some flexibility in risk treatment and budget allocation may be applicable to lower risks, as management may decide to implement specific efficiency measures.

The [Risk Dashboard](#), of which an example is reported in Figure 4 below, is an effective tool to visualise the initial results of the assessment, collecting the emerging risks under the main categories of the taxonomy and representing their classification according to the three tiers and the corresponding colour codes (*red* for very high risks, *orange* for high risks, and *yellow* for medium risks).

Figure 4 – Example of a Risk Dashboard (for illustration purposes only)



Note: The above Risk Dashboard is a representation of a potential outcome from a Risk Assessment and is provided for illustrative purposes only.

If needed to visualise the distribution of risk areas, the Residual Risk Heat Map, a four- quadrant chart as depicted in Figure 5 below, could also provide a graphic representation of the results of the risk assessment, and in particular of the residual risks as a function of risk exposure and level of internal control effectiveness, assisting management in the determination of appropriate risk treatment strategies and risk mitigation measures.

Figure 5 – Example of a Residual Risk Heat Map



Note: The above Residual Risk Map is a representation of a potential outcome from Risk Assessment and is provided for illustrative purposes only.

Tier 1 Risks (Very High)	Tier 2 Risk (High)	Tier 3 Risks (Medium)
1. IT Strategy & System Implementation (3.7.1)	10. Empowerment (2.1.12)	18. Organizational Structure (2.1.5)
2. IT Infrastructure & Systems (3.7.5)	11. Control Environment (2.1.3)	19. Conflicts of Interest (2.2.3)
3. Procurement Requisition (3.4.3.1)	12. Fraud & Illegal Acts (2.2.2)	20. Training (3.5.9)
4. Contract Management (4.1.1.2)	13. Procurement: Bidding & Bid Evaluation (3.4.3.3)	21. Ethics (2.2.1)
5. Accountability (2.1.11)	14. Public Perceptions (2.4.1)	22. Transparency (2.1.9)
6. Procurement Strategy (3.4.3.2)	15. Recruiting, Hiring & Retention (3.5.2)	23. Contract: Administration & Issuance (4.1.1.1)
7. Vendor Management (3.4.4)	16. Performance Measurement (2.1.6)	24. Organizational Synchronization (1.1.7)
8. Resource Allocation & Availability (3.5.1)	17. Budget Allocation (1.1.4)	
9. Strategic Planning (1.1.2)		

5. 3. h Alignment of risks with Mandates, Objectives and Strategic Plans

ERM is driven by organizational strategies and objectives, and the processes and initiatives designed to achieve them. The ability to appropriately link risks to strategies and objectives and the underlying processes and activities is critical to the identification and implementation of effective risk mitigation measures. The template represented in Figure 6 below could support management in this process.

The risk assessment, through the alignment of risks with objectives and plans, effectively facilitates the relationship between the risk management process and budgeting. The output from the risk assessment shall be a key driver and input in supporting decision making around budget priorities and requirements.

Figure 6 – Example of an alignment of risks to objectives (for illustrative purposes only)

Risk Number	Risk Definition	Objectives								
		1	2	3	4	5	6	7	8	9
1.1.2	Strategic Planning	Red	Red	Red	Red	Red	Red	Red	Red	Red
1.1.4	Budget Allocation	Orange	White	Orange	Orange	White	White	Orange	Orange	White
1.1.7	Organizational Synchronization	Yellow	White	Yellow	Yellow	White	White	Yellow	Yellow	Yellow
2.1.3	Control Environment	Orange	Orange	Orange	Orange	White	White	Orange	Orange	Orange
2.1.5	Organizational Structure	Yellow	Yellow	Yellow	Yellow	White	White	Yellow	Yellow	Yellow
2.1.6	Performance Measurement	Orange	Orange	White	Orange	Orange	White	White	White	Orange
2.1.9	Transparency	Yellow	Yellow	White	Yellow	Yellow	Yellow	White	White	Yellow
2.1.11	Accountability	Red	White	White	Red	Red	White	Red	White	Red
2.1.12	Empowerment	Orange	Orange	White	Orange	White	White	Orange	Orange	Orange
2.2.1	Ethics	Yellow	Yellow	White	Yellow	Yellow	White	White	Yellow	Yellow
2.2.2	Fraud & Illegal Acts	Orange	Orange	White	Orange	Orange	White	White	Orange	Orange
2.2.3	Conflicts of Interest	Yellow	Yellow	White	Yellow	Yellow	White	White	Yellow	Yellow
2.4.1	Public Perception, Support , Reputation	Orange	Orange	White	Orange	Orange	White	White	Orange	Orange
3.4.3.1	Procurement: Requisition	Red	Red	Red	Red	Red	Red	Red	Red	Red
3.4.3.2	Procurement: Strategy	Red	Red	White	Red	Red	Red	White	White	Red
3.4.3.3	Procurement: Bidding & Bid Evaluation	Orange	Orange	White	Orange	Orange	White	White	Orange	Orange
3.4.4	Vendor Management	Red	Red	Red	Red	Red	Red	Red	White	White
3.5.1	Resource Allocation & Availability	Red	Red	White	Red	White	White	Red	White	White
3.5.2	Recruiting, Hiring & Retention	Orange	White	White	Orange	White	White	Orange	White	White
3.5.9	Training	Yellow	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow
3.7.1	IT Strategy & Implementation	Red	Red	Red	Red	White	White	White	White	Red
3.7.5	IT Infrastructure & Systems	Red	Red	Red	Red	White	White	White	White	White
4.1.1.1	Contract: Administration & Issuance	Yellow	Yellow	White	White	Yellow	Yellow	White	White	White
4.1.1.2	Contract: Management	Red	Red	White	White	Red	White	White	White	Red

Note: The above alignment of risks to objectives is a representation of a potential outcome from a Risk Assessment, and is provided for illustrative purposes only.

5.3.i Validation workshop

The results of the assessment shall be ultimately validated in a dedicated senior management workshop so that management could share a common understanding of the identified risks, their criticality, and the risk response strategies that should be considered. Senior management workshops at UNEP's corporate level, chaired by the head of entity with the participation of the senior management team, are an essential step in the ERM implementation process, as they contribute to sustain and embed a risk-aware culture at the highest level.

As mentioned before, workshops are an excellent opportunity for sharing risk information, generating enriched conversations on future uncertainties and relevant mitigation strategies. They are conducted under the overall leadership of the head of entity with the facilitation being provided by the ERM function and the Risk Management focal point(s). They cover a central role in the ERM implementation process, directly engaging senior managers in discussions on mandates and objectives, and the risks or uncertainties in effectively achieving them within commonly agreed tolerances. The results of the discussion, aiming to reach consensus on the critical risks, response strategies, and risk ownership, should be fully reflected in the final Risk Register. It is important to note that the final approved Risk Register might differ from the initial draft, as it aims to represent the collegial views of the head of entity and the senior management team.

The Risk Register will include the Risk Universe for the entity (the risk category, sub-category, and risk definition), and further information regarding rating results, risk drivers, and potential risk response strategies. A Risk Register template is attached as [Annex 3](#). The Register should be constantly maintained and updated, reflecting any relevant changes in the risk environment. A formal comprehensive risk assessment shall be undertaken annually.

5.4. Risk Response and Internal Control Activities

Based on the high-level response strategies agreed by senior management and summarized in the Risk Register, Risk Owners shall design a detailed Risk Treatment and Response Plan.

5.4.a Determination of Risk Responses

The quadrant of the Residual Risk Heat Map in which each risk is plotted could facilitate the determination of the proposed risk treatment, broadly falling into four categories:

- i. **Risk Reduction** – Risks characterised by a high-risk exposure and ineffective internal controls will fall in the “risk reduction” quadrant. A reduction in risk exposure could be achieved through different strategies, such as:
 - a. the adoption of *prevention plans* aimed at reducing the likelihood of a risk occurring by treating the risk contributing factors;
 - b. the deployment of *response strategies*, formulating an appropriate risk treatment, should the risk materialise; or
 - c. the *transfer* of risk exposures to external parties through mechanisms as insurance or outsourcing.
- ii. **Risk Acceptance or Optimisation** – Risks falling into this category have a low risk exposure and a level of internal control effectiveness deemed high. Risk may be therefore accepted, as considered either inherent in the environment, or an integral part of the activities necessary to achieve defined objectives.

Other risks may be deemed to be overly controlled, as the level of adopted control measures may reduce the ability of the Organization to effectively achieve stated objectives, or the cost of the internal control activities may be considered to exceed any derived benefits.
- iii. **Risk Monitoring** – Risks with a relatively low risk exposure and low internal control effectiveness will be included in this category. As even if these risks were to materialise, the impact on achievement of objectives would be modest, no improvement in internal control effectiveness would be normally required. The Risk Owner, with support of the local Risk Management Focal Point(s), shall perform regular risk monitoring activities, so that any potential increase of the risk exposure could be timely identified.

- iv. **Internal Control Monitoring** – With regard to the significant risks that are deemed to be appropriately managed, an assessment process effected by the Risk Owner and the local Risk Focal Point, and oversight activities carried out by other monitoring functions, including Internal Audit, shall provide assurance on the ongoing effectiveness of designed internal controls.

5. 4. b **Internal Controls**

As mentioned previously, according to the best international standards, an effective system of internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is deemed to be broader than internal control, expanding and elaborating on internal control to form a more robust conceptualisation and tool for management.

Control activities are an essential part of the process by which UNEP seeks to achieve its objectives. They consist of the policies and procedures that help ensure that management's risk responses are carried out properly and in a timely manner, and include a range of activities, as diverse as approvals, authorisations, verifications, reconciliations, reviews of operational performance, physical controls, and segregation of duties. **Preventive controls** are in particular designed to limit the possibility of a risk maturing and an undesirable outcome being realised. **Detective controls** are conversely designed to identify whether undesirable outcomes have occurred "after the event".

With regard to the identified risks, comprehensive **Risk Treatment and Response Plans** shall outline the main controls management has already established, and the additional control and treatment strategies management plans to introduce to further mitigate risks, as may be appropriate, defining detailed action plans, timelines, and identifying risk treatment owners, as illustrated by Figure 7 below. A Risk Treatment and Response Plan template is attached as [Annex 5](#).

Case study: how UNEP benefits from a Secretariat-wide approach

Implementation of a detailed risk treatment plan for the “Extra-budgetary Funding and Management” risk in the context of UNEP ERM-framework and Secretariat.

The Secretariat-wide Risk Register

The results of the enterprise-wide risk assessment are captured in the UN Secretariat’s Risk Register. Risks are classified into tiers based on the qualitative evaluation of exposures and control effectiveness as well as contributing factors gathered during the risk assessment process. The Management Committee validates the Risk Register to come to a common, shared understanding of risks and their criticality, identifying the risks on which immediate action is needed and the managers (Corporate Risk Owners) responsible for the definition of risk treatment and response plans.

Risk Treatment and Response Plans

The Register is ultimately formally approved by the Secretary-General. In their role, Corporate Risk Owners are supported by Risk Treatment Working Groups, comprised of members of different entities representing the different functional areas of the Secretariat. Members are “subject matter experts” and bring their specialized knowledge to the discussions.

Under the guidance of the respective Corporate Risk Owners, Working Groups define detailed Risk Treatment Plans for each of the critical risks, approved by the Management Committee, as ERM Committee for the Organization, and monitor the work of the responsible risk treatment teams, the effectiveness of the agreed actions in mitigating the risks, and the evolving risk profile of the Organization, with periodic reporting to the Committee.

Extra-budgetary Funding and Management

The Management Committee and the Secretary-General deemed Extra-budgetary Funding and Management as one of the critical risks for the Organization and nominated the Controller as the risk owner at the corporate level. The risk is defined as: “The inability to obtain extra-budgetary funding may impact the ability of certain departments to achieve their objectives. Reliance upon extra-budgetary funding may jeopardize or appear to impact the independence of the UN as projects that obtain earmarked funding may be given higher priority. Inability to identify, establish and maintain the optimal structure and controls for trust funds resulting in loss or misuse of assets.”

Case study

Key drivers include:

- Donors might change priorities or move resources to other actors. Inherent instability of the operations and impact on the ability to plan strategically.
- Reliance on a few donors for a large portion of extra-budgetary funding and lack of predictable funding may be perceived as potentially influencing the Organization to focus on donor countries' priorities and impacting its credibility.
- Loss in extra-budgetary funding will impact the programme support accounts and may also significantly affect the Organization's regular programme of work.
- Delay in anticipated cash against pledges and projected income may impact operations of the Organization negatively.
- Trust fund managers may have limited mechanisms to ensure stewardship of funds by implementing agencies and to enforce proper reporting on the use and impact of funds.
- Potential weaknesses in the establishment and maintenance of adequate controls on the use and impact of funds, and to mitigate fiduciary or corruption risks, could expose the Organization to significant reputational issues.
- Different reporting systems established by donors and inadequate accountability framework may impact the ability to measure the outcomes of XB funded activities.
-

Potential Risk Response strategies involve:

- Development of a comprehensive multi-year resource mobilization strategy. Advocacy for an increase in the number of donor countries.
- Monitoring the effectiveness of systems designed to manage project-related funds; improving the timeliness and comprehensiveness of reporting.
- Holding implementing entities accountable for appropriate use and timely and accurate reporting of the usage of funds.
- Administering and managing extra-budgetary resources with the same rigor as regular budgets.

Case study

The Risk Treatment plan

Under the guidance of the Controller, the dedicated working group defined and implemented a detailed risk treatment plan structured around three main areas:

1. Standardization of donor agreements

- i. Institute Secretariat-wide agreements with key donors
- ii. Issue a clear guidance on restrictive conditions (e.g.: immunities and privileges of the United Nations, single audit principle, procurement, recruitment)
- iii. Establish a set of minimum required clauses for each agreement, such as standardization of donor reports, annual reporting, evaluations, and contribution payment terms

2. Management of implementing partners

- i. Formulate a corporate guidance on standard procedures for selecting implementing partners (IPs), which will clarify the difference between the IP selection process from the procurement process, and between Implementing Partnerships and Grants
- ii. Establish a robust contract management to follow-through funds transferred to IPs
- iii. Make the evaluation of IPs available Secretariat-wide and issue a guidance on how to deal with IPs that do not deliver

3. Update of internal controls mechanisms that govern the administration of trust funds

Update Policies for establishing and managing trust funds (ST/SGB/188 of 1 March 1982) and relevant administrative instructions (ST/AI/284 of March 1982 "General Trust Fund"; ST/AI/285 of March 1982 "Technical Cooperation Trust Funds"; and ST/AI/286 of March 1982 "Programme Support Accounts").

The implementation

As part of the work of the risk treatment group, the Organization issued guidance on restrictive conditions (e.g.: immunities and privileges of the United Nations, single audit principle, procurement, recruitment), and established a set of minimum required clauses for each agreement, such as standardization of donor reports, annual reporting, evaluations, and contribution payment terms. Policies for establishing and managing trust funds (ST/SGB/188) and relevant administrative instructions (ST/AI/284, ST/AI/285) have been updated and circulated to the Secretariat's Finance community.

Corporate guidance on standard procedures for selecting implementing partners (IPs), clarifying the difference between the IP selection process and the procurement process, and between Implementing Partnerships and Grants, is in process of formulation in consultation with programme managers and OLA. The Working Group also analyses proposals to put in place a corporate fraud sanction procedure for implementing partners. The policy is currently being refined, taking into account lessons-learned from other UN agencies.

The implementation of the Working Group's action plan serves as the basis for the Organization's medium-term strategy for further securing and expanding extra-budgetary funding.

5.5. Information and Communication

Relevant risk and internal control information shall be provided to the Executive Office and the Senior Management Team (SMT) within UNEP, to adequately support decision making towards the achievement of established mandates and objectives.

5.5.a UNEP level risk assessment results

The results of the different risk assessments shall be collected by the Administration Unit - Enterprise Risk Management Team and compared within and across UNEP locations. All risk definitions and criteria shall ultimately be aligned to those established at the UNEP HQ level.

Risk results may be compiled and aggregated, as an important input to the Secretariat-wide Enterprise Risk Assessment and Risk Register. The results of the UNEP level assessment shall facilitate UNEP's ability (at both the entity, and the Secretary-General, Management Committee and General Assembly level) to understand and effectively integrate risk assessment outputs into strategic decision-making activities.

5.5.b Results based management

The results of the enterprise risk management process shall be leveraged to support decision-making in strategic planning, budgeting, and allocation of resources. In this perspective, the risk reports described in the following section of this document shall be provided to senior management and governing bodies as part of the reporting and submission phases of the programme planning and budget preparation.

The risk profile of UNEP and the effectiveness of the designed controls shall be fully considered in setting the funding and resource allocation requests as part of the programme planning and budgeting process. An effective enterprise risk management and internal control process will therefore become instrumental to the promotion of a risk driven culture through a more informed risk based decision-making capability, as the significance of risks and the effectiveness of dedicated internal controls will be explicitly considered when evaluating programmes and relevant budget allocations, effectively setting in this process the risk tolerance of UNEP with regard to specific risks and programmes.

5.5.c Risk reporting and frequency

The risks to be reported on, the level of required details, and the frequency of reporting shall depend on the UNEP's target audience. Sufficient information about the risks and associated risk management and internal control activities shall be provided, so that recipients are able to fulfil their risk management responsibilities. Risk and internal control information concerning risks deemed to be of the greatest significance on an Organization-wide basis shall be summarised and provided to the Secretary-General, and through the Secretary-General, the General Assembly and the Advisory

Committee on Administrative and Budgetary Questions (ACABQ) and IAAC, whilst detailed information covering their area of responsibility shall be distributed to the managers responsible for the management of specific risks.

The **frequency** of risk reporting also depends upon the report recipients.

At Secretariat-wide level, *annual reporting* is established to the General Assembly, through the ACABQ and IAAC, whilst *quarterly reporting* is defined for the Management Committee, and through the Management Committee, the Secretary-General. Regarding local level risk registers and risk treatment and response plans, Heads of entity and local senior management teams shall receive *quarterly reports*.

Relevant risk and internal control information shall be provided in line with the reporting and submission phases of the programme planning and budget preparation, where applicable.

In terms of reporting modalities to the ERM Function, **UNEP** will submit our local risk registers through an Interoffice Memorandum addressed to the USG-DMSPC. A notification to the ERM function shall be made through e-mail by the Corporate Services Division's Risk Management Focal Point(s).

UNEP aims to report to the Committee of Permanent Representatives following example of Secretary's General periodical report to the UNGA on the accountability in the United Nations Secretariat⁷.

According to best practices, the annual risk reports that shall be prepared in support of risk management activities take into consideration the following elements.

- i. **UN Secretariat-wide Risk Register** – The Risk Register summarises the most significant risks at Organization level. It includes:
 - (a) Executive summary
 - (b) *Risk Dashboard* - a graphical representation of the significant risks identified as a result of the risk assessment process, and for each risk:
 - (c) Risk definition
 - (d) Risk scoring in terms of impact, likelihood and control / management effectiveness
 - (e) Residual risk classification
 - (f) Factors that contribute to the risk (key drivers)
 - (g) Relevant controls designed by management

⁷ [A/74/658 Review of the efficiency of the administrative and financial functioning of the United Nations](#)

- (h) An overview of the risk response strategy
- (i) Risk ownership
- (j) Strategic Objectives of the Organization [UN Secretariat]
- (k) Secretariat Risk Universe
- (l) Scoring Criteria for the measurement of Impact, Likelihood and level of Control Effectiveness

To facilitate the prioritization and identification of response strategies, risks might as well be charted on a Residual Risk Heat Map.

The Risk Register is formally revised by the Enterprise Risk Management function following the *biennial Secretariat-wide risk assessment* process and distributed to the Management Committee and the Secretary-General. Through the Secretary-General, a summary is distributed to the General Assembly through the ACABQ, and the IAAC.

The Register is constantly monitored and updated to reflect the changing risk profile of the UN Secretariat, as it might be needed, following *quarterly reviews* and discussion at Management Committee level.

- ii. **Risk Register at UNEP level** – Following the same template of the Secretariat-wide Risk Register, the local register will reflect the results of UNEP’s risk assessment. The Risk Register will be distributed to the Executive Director, the Senior Management Team by Corporate Services Division’s Risk Management Focal Point(s), following its formal *periodic (annual) revision*.

The register will be quarterly updated following the discussions of the UNEP Enterprise Risk Management Committee, or as required. Quarterly presentations by the risk owners to the UNEP ERM committee are a powerful tool to ensure the continued attention of the whole senior management team on the most critical risk areas the entity is facing, a prompt identification of significant changes in its overall risk profile, and the consideration of emerging risks. The template of the Risk Register is provided in the ERM’s Community of Practice Site3 and included in [Annex 3](#).

- iii. **UN Secretariat-wide Risk Treatment and Response Plan** – Regarding the most significant risk areas identified, a comprehensive Risk Treatment and Response Plan is prepared by the Risk Owners at corporate-level, considering the advice of dedicated working groups comprised of “subject matter experts”, and approved by the

Management Committee, as Enterprise Risk Management Committee for the Organization. The Risk Treatment and Response Plan summarises the managerial response designed to appropriately mitigate the risks. It includes:


- (a) Executive summary, and for each risk:
- (b) Risk definition, risk scoring in terms of impact, likelihood and control / management effectiveness, residual risk classification and risk ownership
- (c) Risk treatment specific actions
- (d) Due dates
- (e) Responsible teams

Corporate Risk Owners present *quarterly updates* to the Management Committee, on the progress of the implementation of the risk treatment plan and on the evolving nature of the risks under their area of responsibility. Outlines of the Risk Treatment and Response Plan are presented to the General Assembly through the ACABQ, and the IAAC.

- iv. **Risk Treatment and Response Plan at the UNEP level** – Following the same template of the Secretariat-wide Risk Treatment and Response Plan, the local plan reflects the managerial response to the risks identified at UNEP's level. The plans are designed by Risk Owners at the entity-level and approved by [UNEP's ERM Committee](#), which shall then receive *quarterly updates* on progress.

Risk Owners in UNEP may be supported in their responsibilities of defining and implementing risk treatment actions by working groups comprised of thematic experts from across the entity, as deemed appropriate by [UNEP's ERM Committee](#). Corporate Services Division's Risk Management Focal Point(s) shall provide overall coordination and guidance to the process. The template of the Risk Treatment and Response Plan is provided in the ERM's Community of Practice Site⁴ and included in [Annex 5](#).

Figure 7 – Example of a Risk Treatment and Response Plan

5. Extra-budgetary Funding and Management (5.1.2/5.1.4)	Risk category	Impact	Likelihood	Internal Control Effectiveness	Residual Risk	Corporate Risk Owner
	<i>Financial</i>	<i>5 – Critical</i>	<i>4 – Highly likely</i>	<i>3 – Significant improvement needed</i>	<i>Critical</i> 	<i>Controller</i>
Risk Definition	<i>The inability to obtain extra-budgetary funding may impact the ability of certain departments to achieve their objectives. Reliance upon extra-budgetary funding may jeopardize or appear to impact the independence of the UN as projects that obtain earmarked funding may be given higher priority. Inability to identify, establish and maintain the optimal structure and controls for trust funds resulting in loss or misuse of assets.</i>					
Treatment plan	Working Group Members: OPPBA, ECA, Habitat, OCHA, OHCHR, OUSG-DM, UNODC, DESA, Ethics Office					
Risk Treatment Action					Due Date	Responsible Team
1. Standardization of donor agreements						
a. Institute Secretariat-wide agreements with key donors					Dec 2016	OPPBA
b. Issue a clear guidance on restrictive conditions (e.g.: immunities and privileges of the United Nations, single audit principle, procurement, recruitment)					Dec 2015	OPPBA
c. Establish a set of minimum required clauses for each agreement, such as standardization of donor reports, annual reporting, evaluations, and contribution payment terms					Dec 2015	OPPBA
2. Management of implementing partners						
a. Formulate a corporate guidance on standard procedures for selecting implementing partners (IPs), which will clarify the difference between the IP selection process from the procurement process, and between Implementing Partnerships and Grants					Dec 2016	OPPBA
b. Establish a robust contract management to follow-through funds transferred to IPs					Jun 2016	OPPBA
c. Make the evaluation of IPs available Secretariat-wide and issue a guidance on how to deal with IPs that do not deliver					Jun 2016	OPPBA
3. Update of internal controls mechanisms that govern the administration of trust funds						
Update Policies for establishing and managing trust funds (ST/SGB/188 of 1 March 1982) and relevant administrative instructions (ST/AI/284 of March 1982 "General Trust Fund"; ST/AI/285 of March 1982 "Technical Cooperation Trust Funds"; and ST/AI/286 of March 1982 "Programme Support Accounts")					Dec 2015	OPPBA

For illustrative purposes only

Note: The above Risk Treatment and Response Plan is a representation of a potential outcome from a Risk Assessment and is provided for illustrative purposes only.

Note

Escalation of risks beyond the scope of the responsibilities UNEP

As mentioned before, “**Very High**” risks, categorised as *Tier 1* risks at the entity level, shall be reported to the central ERM function. As a result of the risk assessment process, UNEP might as well identify risks for which an effective response should be taken at organization-wide level, and whose management therefore goes beyond the responsibilities of the organizational unit. Such risks should as well be reported to the central ERM function, so that they could be consolidated with other comparable risks emerging in different areas of the Organization, and accordingly reported to the Management Committee, and through the Secretary-General to the IAAC and the General Assembly. Their consideration at the appropriate level allows the Organization to define and implement an adequate corporate level response.

An example could be provided by *Human Resources Strategy and Management* matters. As a result of the entity level risk assessment, departments and offices reported issues as follows:

- The recruitment of qualified and motivated staff and the development of a results and performance-oriented culture are not effectively supported by the existing policies and procedures, hindering the formulation of HR strategies and career planning mechanisms.
- The performance rating system is unable to adequately reflect staff performance.
- Limited consequences are in place to sanction staff and managers for not meeting goals.
- Absence of incentives to reward performance and of opportunities for promotion.
- The Organization’s approach to organizational learning and development is not clearly linked to planning, knowledge management, guidance, training, monitoring and evaluation.

It is evident that an effective response to those issues can be taken only if the risk is managed under the leadership of the USG-DOS and ASG-OHR and the overall guidance of the Management Committee. Regarding those matters, a dedicated working group comprised of thematic experts may be established to progressively review and implement a risk response, including:

- The development of a HR strategy incorporating a stronger talent management element to support a performance-oriented culture.
- Enhancements of workforce planning through the revision of relevant policies and procedures.
- The re-evaluation of the effectiveness of the performance management rating system.
- Rewarding high-performing individuals and teams, considering actions with no financial impact, as well as mechanisms for promotion.
- Holding managers and staff accountable for non-performance against **pre-defined criteria**.

5.6. Monitoring and Assurance

As the environment in which the UN Secretariat operates is constantly changing, the continuous monitoring and review of risk information is crucial to ensure its continued adequacy for effective decision-making. Risk Owners and Risk Treatment Owners will accordingly ensure relevant information remains current or is appropriately re-evaluated in case of specific events or circumstances that could affect the risk profile of their areas of responsibility.

As the risk assessment process relies on management's perception of internal control effectiveness, adequate assurance activities shall as well validate the evaluation, providing assurance regarding the effectiveness of designed controls and the appropriateness of defined risk treatments. The local Risk Management Focal Points and the Corporate Services Division's Risk Management Focal Point(s) shall assist management with ongoing monitoring and reporting.

The **Office of Internal Oversight Services ("OIOS")** will be responsible for the independent evaluation of the effectiveness of the internal control environment, in accordance with its mandate, including the periodic assessment and evaluation of the implementation of an effective enterprise risk management and internal control framework. [Annex 6](#) of this documents list all the UNEP OIOS reports that mention ERM -Risk Management for reference.

The **Board of Auditors**, as part of the assurance activities regarding the financial statements of UNEP described by its charter and mandate, will continue to assess the effectiveness of the system of internal control adopted by UNEP.

5.6.a Enterprise risk management and internal control technology and tools

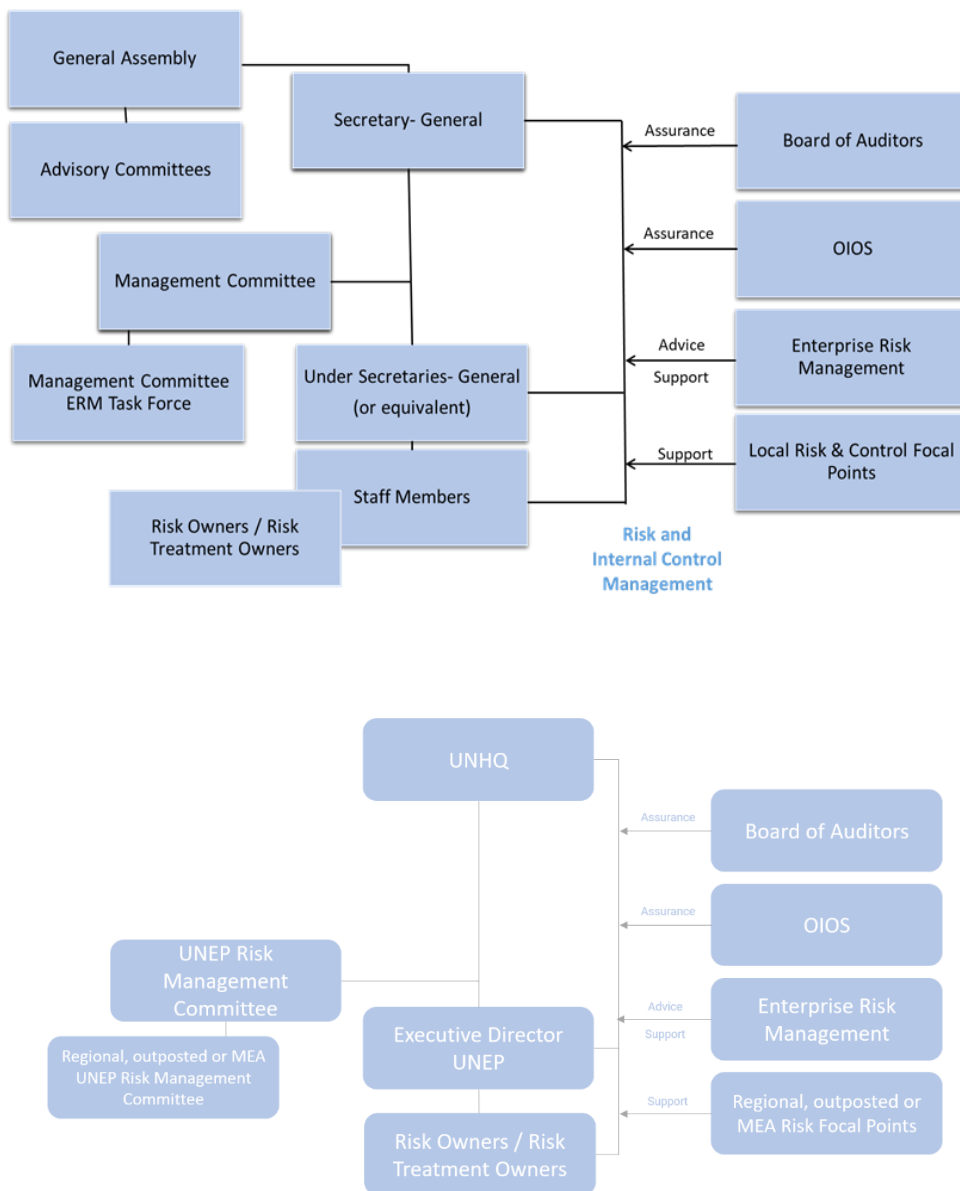
In support of the described enterprise risk management and internal control framework programme, the Secretariat requires the capability to automate many of the activities, tools, and reports critical to the programme's successful implementation. The automation of the framework shall provide a consistent and structured method for identifying, assessing, monitoring, and communicating risks and internal controls associated with the various activities, processes and functions across the Organization.

The IT solution for ERM shall be designed to incorporate the various and diverse elements of the framework, including a linked database repository of risks and risk information (the risk register), and the capability to support and measure risk at different levels within the Organization. The system shall be accessible on a global scale with established access and user rights as defined for each user group and shall have advanced reporting and data management capabilities. DMSPC is expected to roll out a basic information technology tool that will automate the implementation of ERM across the Secretariat – planning to launch in 2021. [Annex 7](#) of this document refers to a software listing of possible ERM tools for UNEP.

6. Risk Governance, Roles and Responsibilities

The Guide has so far presented the definitions of both risk and ERM and introduced the ERM framework that outlines the major steps of the ERM process cycle. This last section will describe the risk governance mechanisms, and the roles and responsibilities of the different functions involved.

Figure 8 – Risk governance structure at Secretariat and at UNEP (Below)



6.1. ERM Leadership at the Secretariat

6.1.a General Assembly

The General Assembly, with the advice of the ACABQ and IAAC, is responsible for determining the risk tolerance of the Organization. The General Assembly covers also a key role in ensuring that senior management adopts and maintains an effective enterprise risk management and internal control framework.

6.1.b Secretary-General

Ultimate responsibility for effective risk and internal control management within the Secretariat resides with the Secretary-General. With the assistance of the Management Committee, the Secretary-General periodically reviews the significant risks facing the Organization, as well as the proposed strategies designed to effectively mitigate the identified risks at a consolidated corporate level, and reports accordingly to the General Assembly and the IAAC.

6.1.c Management Committee

The Management Committee, in its role as the **ERM Committee for the Organization**, provides guidance and direction regarding the implementation of ERM in the Secretariat, and monitors the effectiveness of the overall ERM and internal control framework. In this capacity, the Committee validates the Secretariat-wide Risk Register and come to a common understanding of risks and their criticality and identifies the risks on which immediate action is needed. It further approves the risk governance structure and identifies the managers (Corporate Risk Owners) responsible for the definition of Risk Treatment and Response Plans.

The Committee quarterly reviews the risk profile of the Secretariat and the adequacy of risk response strategies and has an active role in the promotion of the best practices in risk and internal control management in the Organization.

6.1.d Enterprise Risk Management Section in the Department of Management Strategy, Policy and Compliance

Enterprise risk management is the inherent core responsibility of management. Under the framework, embedded risk and internal control management activities are an integral part of the processes and operations of the entire Organization.

Following the Secretary-General's Management reform, the formerly established Enterprise Risk Management function has been reinforced in the Business Transformation and Accountability Division of the Department of Management Strategy, Policy and Compliance (DMSPC) to assist senior management in the process of implementation of the framework. According to best practices and in line with the JIU recommended benchmarks⁶, as well as the non-prescriptive guidelines developed by the High-Level Committee on Management (HLCM) taskforce on ERM⁷, the ERM function strives to integrate ERM in the programme planning processes.

As management is the owner of the identified risks, the ERM section *facilitates* the effective implementation of the ERM framework. It provides assistance to different entities in implementing risk management based on systematic risk mitigation strategies consistently applied across the Secretariat, aggregating risk data from the different organizational units and offices and carrying out regular monitoring of UN Secretariat-wide risks.

The ERM section shall as well facilitate the adoption of consistent methodologies for the assessment of risks throughout United Nations Secretariat, and the implementation of enhanced internal control and risk mitigation measures at the entity level, cooperating with dedicated Risk Focal Points. This process will enable the UN Secretariat to aggregate related risk and internal

control data across the Organization and design the optimal strategies to address the most significant risks to which the UN Secretariat is exposed.

In detail, the main responsibilities of the ERM function in DMSPC include:

- i. Promoting the application of sound risk management *policies*, and providing oversight for the implementation of related activities within the UN Secretariat, defining an overall *vision and direction* for ERM activities.
- ii. Defining a comprehensive ERM *framework* across the Organization to identify, assess, manage and monitor risks and internal controls, supporting the Secretary- General and management in their efforts to embed and sustain risk management activities in the daily operations of the Secretariat.
- iii. Maintaining the *Secretariat-wide Risk Register*, introducing enhancements over time, and coordinating the performance of the risk assessment, holding interviews, developing and reviewing questionnaires, and facilitating workshops, as may be needed.
- iv. Providing the necessary expertise and resources to support the

different steps in the risk management process, including *assistance and advisory* in the design, assessment, and monitoring of appropriate risk mitigation activities and formal Risk Treatment and Response Plans.

- v. Developing and maintaining the *methodology* and practices related to the implementation of risk management activities, including the administration of the tools, training, reporting and other related requirements, and supporting the local Risk Management Focal Points in conducting appropriate risk and internal control monitoring activities.
- vi. Preparing *reports* on risk management activities for distribution to the Management Committee, Secretary-General, and on behalf of the Secretary-General to the General Assembly and the IAAC, as may be required.
- vii. Assisting in the provision of monitoring and oversight of risk management at the entity level, and advising as appropriate on the development and maintenance of local Risk Registers and local Risk Treatment and Response Plans.
- viii. Implementing and maintaining the necessary *information technology (IT) solutions* and data management capabilities to properly support the risk management across the Secretariat entities.
- ix. Supporting the dissemination of information and best practices regarding risk management principles and measures across the Secretariat, and developing as appropriate *communication and training* programs, including websites, e-learning courses and communities of practice, to enhance the Secretariat's risk management culture.
- x. Attending the meetings of the Risk Treatment Working Groups to be held under the leadership of Corporate Risk Owners for the Secretariat-wide Risk Register.

6. 1. e Management Committee ERM Task Force

A Management Committee ERM Task Force composed of Corporate Risk Owners has been created to guide the analysis of the global risks brought by the pandemic in-line with the Secretary General's six Strategic Focus Areas.

As part of its responsibilities and deliverables, the Task Force shall guide the efforts of the Secretariat as follows:

- i. Preparing a detailed analysis pertaining to the Strategic Focus Areas

- identified by the Secretary-General;
- ii. Reviewing the Secretariat-wide Risk Register in the context of the pandemic and ensuring this is detailed and explicit enough to provide a guide to action to the Corporate Risk Owners;
- iii. Preparing a simplified Secretariat-wide Risk Register for senior managers; and
- iv. Ensuring the linkage between the two levels: the overarching priorities of the Secretary-General and the Secretariat-wide Risk Register.

Moreover, the Task Force shall:

- v. Provide advice and guidance in the development and maintenance of the Secretariat-wide Risk Register and Risk Treatment and Response Plans on high-level risks on which the Organization should concentrate its efforts, under the leadership of the respective Corporate Risk Owners;
- vi. Bring their specific experience and expertise to ERM implementation as necessary;
- vii. Monitor the overall risk profile of the Organization and the progress of the corporate risk owners in the implementation of risk mitigation actions; and
- viii. Periodically advise the Management Committee, as the Enterprise Risk Management Committee for the Secretariat, on progress and on future actions for the implementation of ERM in the Organization.

6.2. ERM leadership at UNEP

6.2. a UNEP Executive Director

Under the Secretary General's recently adopted management paradigm, responsibility for the effective implementation of risk management practices, as described by this framework, resides with the respective heads of entities.

As part of the updated Senior Managers' compacts with the Secretary-General, the UNEP Executive Director shall undertake strategic planning based on risk assessment and highlight key risks, and annually confirm their responsibilities for the proper application of the principles and requirements of this framework, and the establishment and maintenance of a strong internal control environment as a result of the risk assessment process.

Further responsibilities include:

- i. Properly considering UNEP's mandate in identification of relevant risks and strategies and implementing a risk management process following the guidelines of the ERM framework.
- ii. Ensuring that risks are correctly identified, managed and monitored, and duly considered in the planning and budgeting process.
- iii. Implementing appropriate risk monitoring and risk treatment plans.
- iv. Providing full support with regard to the implementation of effective risk management and internal control practices, whilst delegating appropriate responsibility for risk and internal control management in accordance with the guidelines established by the framework and supporting policies and procedures.
- v. Reviewing and approving the risk management reports for their area of responsibility and identifying and reporting significant and emerging risks to the Management Committee, and the Secretary-General.
- vi. Developing adequate risk management expertise in their respective areas, ensuring proper participation to relevant training activities.

6.3. ERM drivers at UNEP

6.3.a UNEP's Enterprise Risk Management Committee

The Senior Management Team (SMT) will naturally assume the role of *ERM Committee*, embedding ERM in already established managerial mechanisms. The Committee provides overall guidance and direction regarding the implementation of ERM in the department or office, *quarterly reviews* the local risk profile and the adequacy of risk response strategies and provides relevant advice to the Executive Director and risk owners. [Appendix 4](#) shows terms of reference, composition, frequency of meetings and quorum requirements for local Risk Management Committees.

The Committee is comprised of – at least – the following members:

- i. Deputy Executive Director (chair)
- ii. Chief of Staff, Office of the Executive Director
- iii. Members of the Senior Management Team (SMT)
Directors: CSD and Comms. Division
- iv. Representatives of the Multilateral agreements (MEA's)

6.3.b UNEP Risk Management Focal Points

Corporate Services Division's Risk Management Focal Points are responsible for undertaking and coordinating local risk assessments at UNEP. They will review the progress of the risk assessment, the local level risk register and emerging risks to UNEP operations on a regular basis, as well as take actions to develop and implement risk treatment and response plans to mitigate critical risks.

Corporate Services Division's Risk Management Focal Points⁸ have been formally appointed by UNEP and will continue to liaise with the ERM function in DMSPC to support the implementation of risk assessment and risk and internal control monitoring activities. Responsibilities have been assigned to two existing staff, on a full-time and part-time basis, as deemed suitable by the CSD management considering the complexities of the underlying operations.

More specifically, the responsibilities of UNEP's Risk Management Focal Points include the provision of assistance to UNEP's management in the implementation of the risk management requirements described by this framework, in particular the identification of relevant risks, based on the objectives and mandates of UNEP; the completion of the risk assessment and reporting on its results; the definition of the activities that should be included in the Risk Treatment and Response Plan; and

⁸ Emanuele Corino, Head Administration Unit
Clara E. Stickers, ERM Officer Administration Unit

undertaking monitoring and reporting to senior management on risk management and internal control measures within their area of responsibility.

In addition, UNEP's Risk and Internal Control Focal Points shall customise the Secretariat-wide Risk Universe so that it reflects the risks relevant to UNEP's; prepare reports on all risk management matters, and distribute them to the Enterprise Risk Management function in DMSPC, and the Executive Director of UNEP and local ERM Committee; and monitor the effectiveness of risk management and internal control measures.

6.3.c UNEP Divisional Risk Focal Points and MEA Focal Points

The network of Divisional and MEA Risk Focal Points will assist the implementation of an effective risk management framework in UNEP - in compliance with the UN-Secretariat Enterprise Risk Management and Internal Control (ERM/IC) Policy and Methodology as adopted by the Secretary-General in May 2011.

For the successful implementation of ERM, it is essential that an internal organizational structure with clear roles and responsibilities is established in accordance with the ERM policy and the "three lines of defence" model for ERM:

The third line of defence consists of Senior management, governing bodies and audit and oversight committees and provides assurance and/or assessment of the effectiveness of risk management. Senior management has the ultimate responsibility for managing risks and achieving strategic goals while the Risk Management Committee provides oversight to ensure that senior management is managing risks properly.

The second line of defence is management controls, whereby the ERM team coordinates and oversees risks, assists the first line in ensuring that risks and controls are properly managed, and reports and escalates to the third line of defence: The Risk Management Committee and Senior Management Team.

The first line of defence is formed by the network of Divisional and MEA Risk focal points for which a nomination per Division, Regional Office and MEA is kindly requested.

The Divisional and MEA Risk Focal Points are front-line interlocutors for implementing and supporting ERM processes and will perform the following functions:

- Implementing and supporting the ERM processes across the organization;
- collecting and reporting on risks;
- providing training and updates to staff on risk management policies and processes.

The primary responsibility for identifying risks lies with the MEA Risk Focal Points managers and Business risk owners.

6.4. Risk owners at UNEP

6.4.a Business Risk Owners and Risk Treatment Owners

Business Risk owners are responsible, amongst other matters, for:

- i. Regularly reviewing the risks owned by them, informing UNEP's Risk Management Focal Points of any identified changes, and escalating the risks for which the relevant impact or likelihood is perceived to have increased.
- ii. Determining where internal control deficiencies relating to their risks may be identified, proposing any appropriate risk mitigation measures, and monitoring implementation of risk treatment and response plans relating to risks for which they have responsibility.
- iii. Updating relevant risk information and contributing to risk reporting as may be required.

6.4.b Risk Treatment Working Groups

Risk Owners could be supported in their responsibilities by dedicated working groups comprised of thematic experts from across UNEP, as deemed appropriate by the ERM Committee. The Working Groups, through periodic discussions, will:

- i. Revise the key drivers, the proposed controls and the risk responses.
- ii. Contribute to the definition of Risk Treatment and Response Plans and their implementation under the supervision of the Risk Owners; and
- iii. Bring to the attention of the Risk Owners any emerging issues that might arise during the process.

6.4.c Management and Staff Members

The management of risks and internal controls in accordance with the principles defined by the ERM Policy of the Organization is the responsibility of *all* UN managers and staff members. Defined responsibilities, that will depend on the specific role and function, broadly include:

- i. Embedding risk management in strategic and operational decision making, identifying, managing and monitoring risks with regard to day-to-day operations within the areas of responsibility.
- ii. Providing oversight on the appropriate application of risk management methodologies by the staff members reporting to them, where relevant.
- iii. Monitoring the efficiency and effectiveness of defined control and risk mitigation measures, and contributing to the planning and budgeting process with regard to risk management matters, if applicable.
- iv. Escalating risks as it may be appropriate, and providing timely and accurate risk information to Risk Owners, Risk Focal Points, and the ERM function.
- v. Providing support to the implementation of Secretariat's ERM framework.

6.5. ERM Oversight and accountability at UNEP

6.5.a Office of Internal Oversight Services

In accordance with its mandate, the Office of Internal Oversight Services shall continue to be responsible for evaluating the effectiveness of the internal control environment, including the periodic assessment and evaluation of the implementation of an effective ERM framework.

The Office of Internal Oversight Services is as well responsible for the review of the results of the risk assessments process, and shall consider its outcomes into its audit planning exercise, as deemed appropriate.

6.5.b Joint Inspection Unit

The Joint Inspection Unit, as the oversight body of the United Nations system mandated to conduct system-wide evaluations, shall identify enterprise risk management and internal control best practices, propose benchmarks, and facilitate information-sharing throughout the system.

6.5.c Board of Auditors

The Board of Auditors, as part of its assurance activities on the financial reporting of UNEP, is expected to utilise the results of the risk assessment as an important element of its evaluation of UNEP's system of internal controls, as described by its mandate.

7. Final Provisions

- i. These guidelines shall be implemented in a phased and orderly manner with the aim to optimize and realize the full benefits of the ERM framework. The estimated implementation time path can be found UNEP ERM Implementation Roadmap [Appendix 5](#) and elaborate Timetable – [Annex 8](#).
- ii. Full completion of the implementation cycle is targeted by 30 July 2022.
- iii. UNEP recognizes that ERM is not a 'one size fits all' approach. The key is to determine the degree of maturity that is right for the Organisation and the specific needs of senior management to tailor - while maintaining full compliance to the Secretary-General's policy - an ERM/IC programme that is appropriate for UNEP.
- iv. Various parallel exercises have been planned to enhance the scope of risk management within UNEP such as the Statement of Internal Control (SIC, the Risk Appetite Statement (RAS) and the Reference Maturity Model for Risk Management (RMM). More information can be found in [Annex 9](#) of this document.
- v. ERM is a continuous improvement process and this document will evolve accordingly.

Appendices

Appendix 1: Glossary of Terms and Definitions ⁸

Term	Definition
Control Effectiveness	A measure of how reliably the internal control operates.
Enterprise Risk Management	The process of coordinated activities designed to direct and control an organization with regard to risk, the effect of uncertainty on objectives. It is effected by governing bodies, management and other personnel, and applied in strategy-setting throughout the Organization. Internal control is encompassed within and an integral part of enterprise risk management.
Internal Control	A process, effected by governing bodies, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.
Impact	Result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity's related objectives.
Largest Credible Risk	Risk Exposure in the case of simultaneous failure of several controls established to mitigate the risk.
Likelihood	The possibility that a given event will occur.
Reasonable assurance	The concept that enterprise risk management, even if well designed and operated, cannot provide a guarantee regarding the achievement of an entity's objectives, due to the limitations of the human judgement; resource constraints and the need to consider the cost of controls in relation to expected benefits; and the possibility of management override and collusion.
Residual Risk	The remaining risk after management has taken action to alter the risk's likelihood or impact.

⁸ Consistent with the best international standards, as "Enterprise Risk Management - Integrated Framework" and "Thought Papers on Enterprise Risk Management", Committee of Sponsoring Organizations of the Treadway Commission, 2017;

"Guidelines for Internal Control Standards for the Public Sector", Internal Control Standards Committee of the International Organization of Supreme Audit Institutions, 2004 and 2007;

"Risk management – Principles and Guidelines" – International Organization for Standardization, 2018";

"Reference Maturity Model for Risk Management (CEB/2019/HLCM/25); and Guidelines on Risk Appetite Statements (CEB/2019/HLCM/26)".

Term	Definition
Residual Risk Heat Map	Risk Exposure and Internal Control Effectiveness Matrix – Overview of the Organization’s main risks. Typically, a four or multi-quadrant chart is used to display risk assessment results, as a function of Risk Exposure and Level of Risk Mitigation Activities or Internal Control Effectiveness.
Risk	The effect of uncertainty on objectives.
Risk Appetite	Risk Appetite can be defined as the aggregate amount of risk an organisation seeks to assume in pursuit of its strategic objectives and mission.
Risk Dashboard	Summary of the significant risks identified as a result of the risk assessment process. Composite of the risks that have been assessed to the most important to the Organization.
Risk Exposure	Magnitude of a risk measured in terms of the combination of Impact and Likelihood.
Risk Register	Central repository of all risks and risk information maintained by the Organization, including the risk category, sub-category, risk, risk definition, rating results, contributing factors, and other relevant information pertaining to that risk.
Risk Tolerance	Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives; or put another way the boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long-term objectives.
Risk Universe, or Risk Catalogue	High level description of all the risks relevant to the Organization, including the risk category, sub-category, risk and risk definition.
Tier 1 Risks	Very High Risks – Risks perceived to be of greatest importance based on relative level of significance to the Organization and location, and that require the most attention.
Tier 2 Risks	High Risks – Risks which may require dedicated focus and specific remedial action.
Tier 3 Risks	Medium Risks – Other risks determined to have a medium exposure, and that might require specific remedial or monitoring measures.

Appendix 2: United Nations Secretariat-wide Risk Universe

United Nations Secretariat Risk Universe

1 STRATEGIC	2 GOVERNANCE	3 MANAGERIAL	4 OPERATIONS	5 FINANCIAL	7 FRAUD and CORRUPTION
1.1 Planning	2.1 Governance	3.1 General Management	4.1 Support Services	5.1 Funding and Investments	7.1 Fraud Control Environment
1.1.1 Vision and Mandate	2.1.1 Tone at the Top	3.1.1 Mgmt of Org. Transformation	4.1.1 Translation and Interpretation	5.1.1 Financial Contributions	7.1.1 Organizational Culture & Envirmnt
1.1.2 Strategic Planning	2.1.2 Control Environment/ Risk Mgmt	3.1.2 Leadership and Management	4.1.2 Procurement	5.1.2 Extra-budgetary Funding	7.1.2 ICT Governance & Cyber Security
1.1.3 Budgeting	2.1.3 Organizational Structure	3.1.3 Staff/Management Relations	4.1.3 Supplier Management	5.1.3 Trust Fund Management	7.1.3 Umoja System Control Envirmnt
1.1.4 Budget Allocation	2.1.4 Transparency		4.1.4 Asset and Inventory Management	5.1.4 Donor Fund Mgmt & Reporting	
1.1.5 Prog Performance Measurement	2.1.5 Accountability	3.2 Programme Management	4.1.5 Facilities and Real Estate Mgmt	5.1.5 Cash Management	7.2 Programme Delivery
1.1.6 Planning Execution & Integration	2.1.6 Empowerment	3.2.1 Advocacy	4.1.6 Capital Master Planning	5.1.6 Investments	7.2.1 Political Influence on Prog Reprtnq
1.1.7 HR Strategy and Planning	2.2 Ethical behaviour	3.2.2 Outreach Activities	4.1.7 Business Continuity	5.1.7 Financial Markets	7.2.2 Implementing Partners
1.1.8 Organizational Synchronization	2.2.1 Ethics	3.2.3 Economic and Social Development	4.1.8 Commercial Activities	5.1.8 Insurance	7.2.3 Contingent-Owned Equipment
1.1.9 Outsourcing	2.2.2 Sexual Exploitation and Abuse	3.2.4 Research, Analysis and Advisory			7.2.4 Theft: Fuel, Relations, Inventory
1.1.10 Org. Transf.n & Mgmt Reform	2.2.3 Professional Conduct	3.2.5 Human Rights	4.2 Human Resources	5.2 Accounting and Reporting	
	2.2.4 Sexual Harasment	3.2.6 Humanitarian Assistance	4.2.1 Resource Allocation & Availability	5.2.1 Financial Mgmt and Reporting	7.3 Human Resources
1.2 Principal Organs, Partners	2.3 Communications and PR	3.2.7 Disarmament	4.2.2 Recruiting, Hiring and Retention	5.2.2 General Accounting	7.3.1 Educational/Professional Creds
1.2.1 GA and Member States	2.3.1 Media Relations and PI	3.2.8 Combatting Terrorism	4.2.3 Training and Development	5.2.3 Financial Controls	7.3.2 Recruitment
1.2.2 Partners and Donors	2.3.2 Crisis Communications	3.2.9 Crime Prevention/Drug Control	4.2.4 Performance Management	5.2.4 Liability Management	7.3.3 Payroll: Attendance, Travel, Leave
1.2.3 Inter-Agency Coordination	2.3.3 Internet, Soc Media, Radio, TV	3.2.10 Policy Development	4.2.5 Succession Planning & Promotion	5.2.5 Steff Tax Reimbursements	7.3.4 Benefits and Allowances
	2.3.4 Technology Communication	3.2.11 Inter-agency Programme Coop.	4.2.6 Mobility		7.3.5 Medical Insurance
1.3 Internal & External Factors		3.2.12 Conference Management	4.2.7 Compensation and Benefits		7.3.6 Gifts, Entertainment, Travel
1.3.1 Political Climate - External			4.2.8 Discipline and Conduct		7.3.7 Conflicts of Interest
1.3.2 Political Climate - Internal		3.3 Mission activities	4.2.9 Healthcare Management		
1.3.3 Economic Factors - Commodity		3.3.1 Peacekeeping/SPM Mandates	4.2.10 Occupational Safety and Health	6 COMPLIANCE	7.4 Central Services
1.3.4 Unique Events (i.e. Pandemic)		3.3.2 Electoral Support	4.2.11 Security	6.1 Legal	7.4.1 Procurement
1.3.5 Climate Change		3.3.3 Rule of Law		6.1.1 Contract	7.4.2 False Statements & Laissez Passer
		3.3.4 Mission Planning	4.3 Intellectual Property	6.1.2 Intellectual Property	
1.4 Reputation		3.3.5 Mission Start-up	4.3.1 Knowledge Management	6.1.3 Anti-Corruption	
1.4.1 Public Perception & Reputation		3.3.6 Mission Liquidation	4.3.2 Information and Document Mgmt	6.1.4 International Law	
1.4.2 Crisis & Contingency Mgmt		3.3.7 Logistics		6.1.5 Privacy	
		3.3.8 Air, Lend and Sea Operations	4.4 Information Resources & IT		
		3.3.9 Engineering	4.4.1 IT Strategy	6.2 Regulatory	
		3.3.10 Communications	4.4.2 IT Security and Access	6.2.1 Internal Policies and Resolutions	
		3.3.11 Mission staffing	4.4.3 IT Availability and Continuity	6.2.2 UN Labour Relations	
		3.3.12 Mission Creep	4.4.4 IT Integrity	6.2.3 Host country regulations	
			4.4.5 IT Infrastructure		
		3.4 International tribunals			
		3.4.1 Investigations and Prosecution	4.5 Environmental Sustainability		
		3.4.2 Triels and Appeals	4.5.1 Environmental Management		
		3.4.3 Legal Aid			
		3.4.4 Court Mgmt & Legal Support			
		3.4.5 Witness Protection			
		3.4.6 Detention Unit Management			
		3.4.7 Completion Strategy			
		3.4.8 Residual Capacity and Activities			

Appendix 3: Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control

Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness Impact

Score	Rating	Description of impact						Recovery
		Safety and security	Duration	Organizational and operational scope	Reputational impact	Impact on operations	Financial impact (measured in terms of budget)	Required action to recover
5	Critical	Loss of life (staff, partners, general population)	Potentially irrecoverable impact	Organization-wide: inability to continue normal business operations across the Organization.	Reports in key international media for more than one week	Inability to perform mission or operations for more than one month	>5 per cent >\$500 million	Requires significant attention and intervention from General Assembly and Member States
4	Significant	Loss of life due to accidents/non-hostile activities	Recoverable in the long term (i.e., 24-36 months)	Two (2) or more departments/offices or locations: significant, ongoing interruptions to business operations within 2 or more departments/ offices or locations	Comments in international media/forum	Disruption in operations for one week or longer	3-5 per cent \$300 million-\$500 million	Requires attention from senior management
3	High	Injury to United Nations staff, partners and general population	Recoverable in the short term (i.e., 12-24 months)	One (1) or more departments/offices or locations: moderate impact within one or more departments/offices or locations	Several external comments within a country	Disruption in operations for less than one week	<2-3 per cent \$200 million-\$300 million	Requires intervention from middle management
2	Moderate	Loss of infrastructure, equipment or other assets	Temporary (i.e., less than 12 months)	One (1) department/office or location: limited impact within department/office or location	Isolated external comments within a country	Moderate disruption to operations	<1-2 per cent \$100 million-\$200 million	Issues delegated to junior management and staff to resolve
1	Low	Damage to infrastructure, equipment or other assets	Not applicable or limited impact				<1 per cent <\$100 million	Not applicable or limited impact

Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness

Likelihood

Score	Rating	Certainty	Frequency
5	Expected	>90 per cent	At least yearly and/or multiple occurrences within the year
4	Highly likely	<90 per cent	Approximately every 1-3 years
3	Likely	<60 per cent	Approximately every 3-7 years
2	Unlikely	<30 per cent	Approximately every 7-10 years
1	Rare	<10 per cent	Every 10 years and beyond or rarely

Level of Internal Control / Management Effectiveness

Score	Rating	Description
5	Effective	Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks
4	Limited improvement needed	Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified
3	Significant improvement needed	Key controls and/or management activities in place, with significant opportunities for improvement identified
2	Ineffective	Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and are somewhat ineffective in efficiently mitigating risk or driving efficiency
1	Highly ineffective	Controls and/or management activities are non-existent or have major deficiencies and do not operate as intended. Controls and/or management activities as designed are highly ineffective in efficiently mitigating risk or driving efficiency

Appendix 4: UNEP Risk Management Committee Terms of Reference

UNEP Risk Management Committee Terms of Reference

Mandate

In accordance with the Secretariat's Enterprise Risk Management policy, UNEP's Executive Director is responsible for the effective implementation of risk management. UNEP's Executive Director shall constitute a *UNEP Risk Management Committee*, the Senior Management Team (SMT) to align and coordinate activities related to risk management matters.

The Committee shall serve as a forum to build consensus on key strategic areas by validating and prioritizing risks; identifying trends and emerging risks; and reviewing and recommending measures to proactively manage risks.

Functions of the Local Risk Management Committee

Reporting to the Executive Director and Senior Management Team (SMT), the Committee will perform the following functions:

- i. Validate and prioritize risks identified across the entity and determine the risks to be reflected in the risk register; and escalate any issues to the Senior Management Team (SMT);
- ii. Ensure the alignment of the risk management framework with the Secretariat-wide Policy and Methodology;
- iii. Review the final Risk Register prior to submission for approval to the Executive Director;
- iv. Perform ongoing reviews and updates of the Risk Register and identify emerging risks, and determine the risks to be added or downgraded from the risk register;
- v. Submit the consolidated plan of risk treatment measures to the Executive Director and escalate any issues to the Senior Management Team (SMT);
- vi. Deal with any other relevant risk management and internal control matters.

The Committee is comprised of – at least – the following members:

- v. Deputy Executive Director (chair)
- vi. Chief of Staff, Office of the Executive Director
- vii. Members of the Senior Management Team (SMT)
Directors: CSD and Comms. Division
- viii. Representatives of the Multilateral agreements (MEA's)

The local ERM committee shall be composed of the Senior Management team of UNEP, including the Corporate Services Division's Risk Management focal points as the **Secretariat of the Committee**.

Frequency of meetings and Quorum

The Committee shall meet at least quarterly to assess and validate risks and review the adequacy and effectiveness of risk mitigation measures as detailed in the consolidated risk treatment plan.

A meeting shall be considered as duly constituted when majority of the members are present.

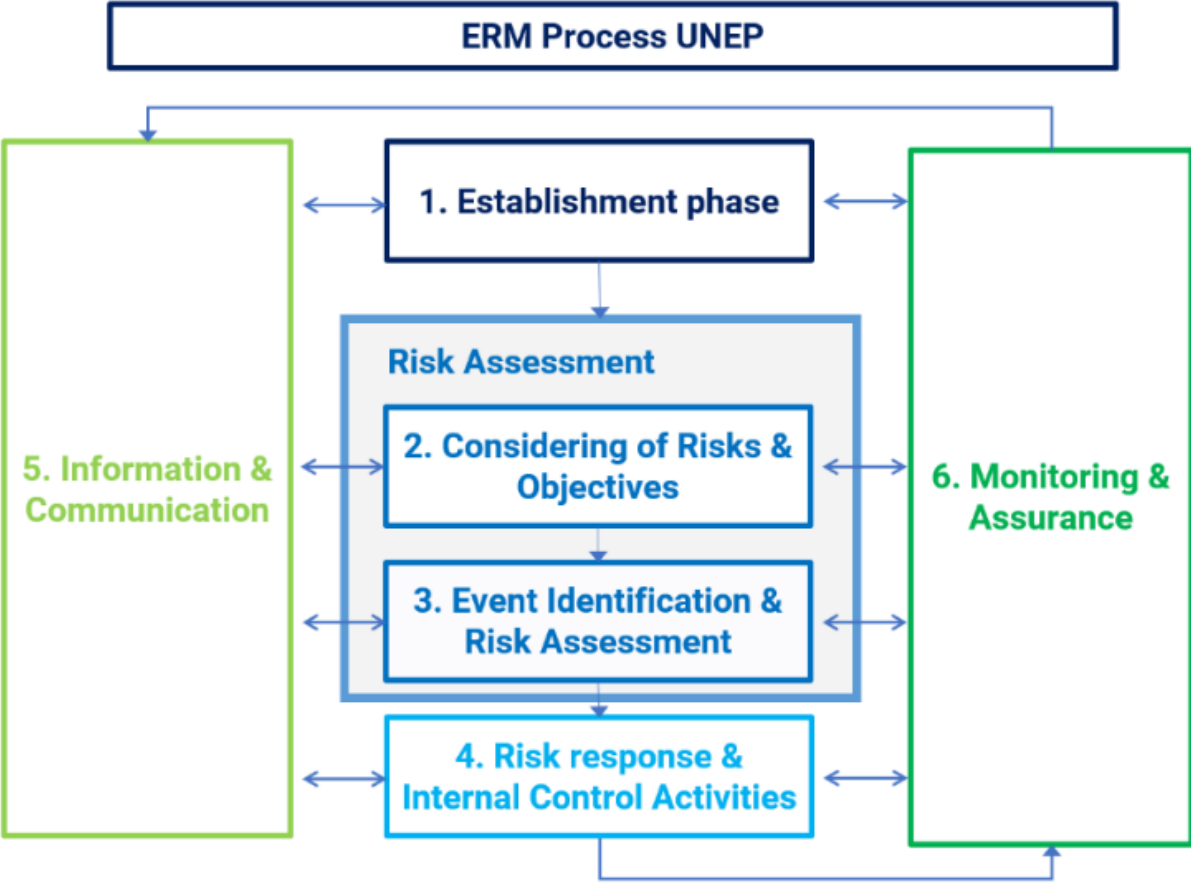
The Committee shall maintain a written record of the main issues and recommendations discussed during the meeting.

Appendix 5: Phased Implementation and Implementation Roadmap

The ERM framework will be implemented in phases with some activities taking place in parallel sequences in order to optimize the full benefits of the exercise. The end of the implantation cycle – after the first feedback loop - is target at the end of 202. Full implantation of the Framework is set for May 2022. Phases of ERM implementation are:

Phase	Implementation	Q3 2021	Q4 2021	Q1 2022	Q2 2022	Q3 2022	Q4 2022
1 – Establishment	Draft and endorsement of ERM framework	■					
	ERM Sensitisation period	■	■				
2&3 – Risk Assessment	Identification and assessment of corporate level risks	■				■	
	Validation of priority risks	■	■				
	Statement Internal Control (SIC)			■		■	
4 – Risk Response & Internal Control Activities	Design of Treatment and Response (TR)		■	■			
	Implementation of TR-plans			■	■	■	■
6 – Monitoring & Assurance	Monitoring and feedback loop				■	■	■
5 – Information & Communication	ERM Training	■					
	Periodic Risk Reporting		■	■	■	■	■

ERM Process at UNEP



8. Annexes

- Annex 1: [UN Secretariat Enterprise Risk Management and Internal Control Policy – 2011](#)
- Annex 2: [UN Secretariat Enterprise Risk Management and Internal Control Guide for Managers - 2020](#)
- Annex 3: [UNEP's Risk Assessment and Universe 2014](#)
- Annex 4: [UNEP Sample Questionnaire and Sample Survey](#)
- Annex 5: Templates: [Risk treatments plan, risk register, residual risk calculator.](#)
- Annex 6: [List of all UNEP OIOS reports that mention ERM and executive summary of recommendations.](#)
- Annex 7: [ERM software listing](#)
- Annex 8: [UNEP ERM Implementation Timetable](#)
- Annex 9: [SIC – RAS – RMM](#)

