



## INTERNAL AUDIT DIVISION

### REPORT 2017/115

---

Advisory review of the implementation  
of the Enterprise Risk Management  
Policy and Procedures at the Office of  
the United Nations High Commissioner  
for Refugees

2 November 2017  
Assignment No. VR2017/160/02

# CONTENTS

	<i>Page</i>
I. INTRODUCTION	1
II. OBJECTIVE, SCOPE, METHODOLOGY AND APPROACH	1-2
III. RESULTS OF THE ADVISORY ENGAGEMENT	2-4
V. ACKNOWLEDGEMENT	5
APPENDIX I Management response	

# **Advisory review of the implementation of the Enterprise Risk Management Policy and Procedures at the United Nations High Commissioner for Refugees**

## **I. INTRODUCTION**

1. The Office of Internal Oversight Services conducted an advisory engagement on the status of the implementation of the Enterprise Risk Management Policy and Procedures at the Office of the United Nations High Commissioner for Refugees (UNHCR).

2. In 2006, the United Nations General Assembly endorsed the adoption of Enterprise Risk Management (ERM) in the United Nations system. In 2011, the Board of Auditors recommended that UNHCR implement ERM as a matter of urgency. Subsequently, UNHCR created an Enterprise Risk Management Unit in 2013. The Unit is headed by a Chief Risk Officer who reports directly to the Deputy High Commissioner. UNHCR formally launched its organization wide ERM Framework through the Policy for Enterprise Risk Management in UNHCR (UNHCR/HCP/2014/7) in July 2014. This was followed by detailed Administrative Instructions and Procedures for Implementation of Enterprise Risk Management in UNHCR (UNHCR/AI/2014/22) in December 2014. The main purpose of the ERM Framework was to enhance risk informed decision making in the organization supported by systematic and structured risk analysis and treatment. The UNHCR ERM Framework was based on the international standard for risk management set out by the International Organization for Standardization (ISO) in ISO 31000, Risk management – Principles and guidelines.

3. The principle responsibility for risk management rests with the Representatives in field operations and the Directors at headquarters, in their capacity as risk owners. UNHCR captures risk information in two risk registers; the Corporate Risk Register, which contains information about risks managed by individual field operations and headquarters entities, and the Strategic Risk Register, which contains key organization wide risks. UNHCR completed its first organization wide risk assessment in April 2015 with mandatory annual risk reviews taking place in November each year. Each risk register is supposed to identify risks as well as treatments to mitigate those risks. The Strategic Risk Register was initially developed in 2014 and approved by the High Commissioner in January 2015. The ERM Unit maintains the Corporate Risk Register and the Strategic Risk Register as well as the overall ERM Framework and associated risk management methodologies. It is also responsible for promoting sound risk management, developing training and communication programmes to enhance the risk culture of UNHCR, providing support to risk owners, analyzing risk data, and providing updates on ERM to governing bodies. The Unit supports risk management processes through organization wide monitoring, reporting and trend analysis. UNHCR has planned to review its Policy and Administrative Instructions and Procedures on ERM in 2017 to validate or revise the adopted concepts and processes and reflect on lessons learned.

## **II. OBJECTIVE, SCOPE, METHODOLOGY AND APPROACH**

4. The objective of the advisory engagement was to inform UNHCR senior management of the status of ERM implementation in the organization and provide options and suggestions for the revision of the ERM Framework.

5. The advisory engagement was included in the 2017 internal audit work plan of OIOS following a request from UNHCR to review its implementation of ERM, in order to inform the planned UNHCR review of the ERM Framework in 2017.

6. OIOS conducted this advisory engagement from March to June 2017. The engagement covered the period after the entry into force of the ERM Policy on 1 August 2014 until 30 June 2017. The terms of reference for the advisory were discussed and agreed with the ERM Unit and approved by the Deputy High Commissioner. The terms of reference identified 15 key review questions for OIOS to address. These questions related to the effectiveness and utility of the ERM Framework overall and the Corporate Risk Register and Strategic Risk Register particularly. The key review questions also covered whether the UNHCR ERM Framework should be expanded to cover certain additional concepts, such as risk appetite and tolerance and more structured opportunity analysis.

7. In order to answer the 15 key review questions, OIOS developed and implemented a data collection and analysis approach comprising the following elements:

- Interviews with risk owners in the field and headquarters including Representatives, Bureau Directors, and Division Directors. Field operations were selected to give wide geographical coverage and to include a variety of different operational contexts (emergency responses, protected situations, planned operational disengagement, etc.) following consultation with the ERM Unit.
- Interviews with three Senior Executive Team members concerning the management of strategic risks and the ERM Framework overall.
- An anonymous electronic survey sent to all 385 risk owners and risk management focal points registered as users of the online corporate risk register (150 of them completed all questions).
- Benchmarking and comparison of the ERM implementation with three other United Nations agencies and one non-United Nations international organization following interviews with their staff responsible for ERM and review of their policies.
- Analytical review of a statistically significant sample of 330 out of 2,365 approved risks in the Corporate Risk Register as of 21 March 2017.
- Desk reviews of official guidance, reference and learning material.
- Qualitative analysis of the Strategic Risk Register.
- Analysis of information from the OIOS field audits conducted in 2016 and the first half of 2017.

8. The engagement was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

### **III. RESULTS OF THE ADVISORY ENGAGEMENT**

9. Three years after its adoption by UNHCR, the ERM Framework is firmly in place and has gained acceptance although it is yet to fully permeate the organizational culture. ERM is widely accepted as a reality and while there remains some resistance to it, the majority of staff and managers see value in the Framework. All operations in the field, as well as Divisions and Bureaux at the headquarters, have created risk registers and reviewed them at least twice. Strategic risks have been identified and discussed at the most senior level within the organization. More than 1,000 staff members have taken e-learning on ERM and a further 184 have been trained in person. The external governance bodies consider UNHCR's ERM implementation in a positive light.

10. Nevertheless, there remains scope for improving the ERM Framework as UNHCR becomes more accepting of it and more risk mature over time. OIOS identified 12 areas for improvement.

11. To address issues identified in the engagement concerning **ERM within UNHCR governance structures**, UNHCR could consider:

- Determining the roles of the Senior Management Committee and Senior Executive Team with regards to the ERM Framework and the Strategic Risk Register and ensuring that they become a regular agenda item for the meetings of both these bodies.

12. To address issues identified in the engagement concerning the **management of strategic, organization wide risks**, UNHCR could consider:

- Developing a dashboard report of the Strategic Risk Register that highlights critical information and recent changes for the attention of senior management. This report could be regularly submitted to the Senior Executive Team and the Senior Management Committee for their consideration and action;
- Disseminating the dashboard report, or an edited version of it, to all risk owners on a regular basis to inform them of risks that may occur or risk responses that may have an indirect effect on activities under their purview;
- Identifying sources of information and associated analysis needed for senior management to make informed decisions on the identification and management of strategic risks. This information and analysis could be collated periodically by the ERM Unit and presented to senior management. The information could include indicators derived from financial data, results from oversight bodies, performance information from the results framework, the Corporate Risk Register, and other sources; and
- Making it a requirement in the revised Policy on the Development, Management and Dissemination of UNHCR Internal Guidance Material that during the proposal, drafting and consultation stage and at the approval and registration stage, an assessment is made whether the proposed internal guidance is addressing key risks articulated in the Strategic Risk Register. Criteria could be established as to when internal guidance can be issued without it addressing risks in the Strategic Risk Register.

13. To address issues identified in the engagement concerning the **management of risks at the Division, Bureau and field operation level**, UNHCR could consider:

- Assessing what management information it wishes to obtain from the Corporate Risk Register, who should receive this information, in what format, and how frequently, in order to better demonstrate the added value of ERM to as wide a range of internal stakeholders as possible;
- Clearly defining in the Policy on ERM the responsibilities of the Bureaux with regards to the monitoring and quality assurance over risk management in the operations within their purview;
- Including a field in the Operations Plan which requires operations to summarize the outputs of their ERM analysis and discuss how this relates to their prioritized operational results; and
- Including a second mandatory risk review in March each year and requiring field operations to report on ERM at mid-year and year-end.

14. To address issues identified in the engagement concerning the **application and effectiveness of the Corporate Risk Register**, UNHCR could consider:

- Including in the Policy on ERM a commitment to keep risk categorization under regular review and to amend the categories prior to the launch of the revised results framework based on the following criteria: the risk categories should: a) support risk owners in effectively managing their risks; b) support the ERM Unit in producing desired management information to inform corporate level analysis and management of overall risk trends; and c) be clearly aligned with the revised results framework to support the management of risks to the achievement of organizational goals;

- Issuing additional guidance clarifying how risks should be categorized in the event that: a) the risk trigger, event and impact relate to different categories; or b) the entire risk could logically be placed under multiple different categories; and
- Either removing the concept of ‘priority risks’ from the ERM Framework and instead prioritize risk responses based on the risk rating, or issuing clear guidance explaining the basis upon which priority risks should be selected.

15. OIOS considers that implementing the above suggested improvements would strengthen risk management and culture in UNHCR and further embed ERM in its operations. **OIOS suggests that UNHCR senior management identifies areas it wishes to implement and the level of risk maturity it wishes to reach and sets target timelines for achieving these.** Doing so would ensure that the momentum currently behind ERM will not be lost. OIOS notes that the ISO 31000 standard is currently undergoing revision and an updated standard is expected to be issued late in 2017 or early 2018. Given this, **OIOS suggests that the revision of the UNHCR Policy on ERM and any action taken on the suggested improvements in this advisory report are done with due consideration to the revised ISO 31000.**

16. With regards to introducing the concept of risk tolerance, as well as the underlying concept of risk appetite, OIOS is of the opinion that at this stage of implementation of the ERM Framework it could have the potential to backfire and create more confusion rather than clarifying management’s view of risk. Further, setting tolerance levels in a clear and appropriate manner with regards to the work of UNHCR is a complex and challenging exercise that would require extensive attention from the organization at a time when senior management has many urgent competing priorities. As the maturity of ERM improves in UNHCR, a formal statement on risk appetite and tolerance in the Policy on ERM could be considered. In the long term this would support management in determining the effectiveness of risk management. However, at this moment **OIOS encourages UNHCR to instead continue implicitly applying the concept of risk tolerance in the design of specific policies where appropriate, on a case by case basis. In addition, UNHCR could give consideration to the level of risk that management is willing to accept in relation to select key organizational risks and ensure that risk treatments reflect this consideration.**

17. With regards to more explicit capturing and analysis of opportunities, in the opinion of OIOS, formally capturing opportunities within both the Corporate and Strategic Risk Registers would assist UNHCR in identifying, analyzing and exploiting opportunities in a more structured and holistic manner. OIOS is further of the opinion that doing so would not add excessive complexity or bureaucracy to the ERM framework and could also improve the risk culture within UNHCR. **UNHCR could include opportunity analysis in its Corporate and Strategic Risk Registers after proper conceptualization and piloting with linkages to its programme planning for exploiting the identified opportunities.**

18. OIOS acknowledges the concerns that UNHCR is dealing with a wide range of organizational pressures and changes. The field operations particularly often feel as though they are barely able to keep pace with the various initiatives, policies and requirements developed centrally. However, in the view of OIOS, ERM is a key tool to help UNHCR deal with these various demands in an informed, risk aware and effective manner. The stronger the ERM Framework becomes, the better able UNHCR should be to prioritize amongst competing demands and achieve its objectives. OIOS is also of the view that the more integrated ERM is into the operations management cycle, the more its benefits will be realized and the less it will be considered as additional work. This requires that the internal governance structures continue to regularly review and revisit the Framework to make it a useful and integrated tool in guiding managerial decision making and prioritization. Ultimately, ERM should become an embedded, natural part of existing procedures rather than a standalone activity. The review of the ERM Framework is an opportunity for UNHCR to build on the progress achieved to date and to refine and improve its risk management processes, leaving it better equipped to deliver its mandate.

#### **IV. ACKNOWLEDGEMENT**

19. OIOS wishes to express its appreciation to the management and staff of UNHCR for the assistance and cooperation extended to the auditors during this assignment.

*(Signed)* Eleanor T. Burns  
Director, Internal Audit Division  
Office of Internal Oversight Services

# **APPENDIX I**

## **Management Response**






**UNHCR**  
United Nations High Commissioner for Refugees  
Haut Commissariat des Nations Unies pour les réfugiés

## Memorandum

**UNHCR**

Case postale 2500  
CH-1211 Genève 2

To: Mika Tapio, Chief, UNHCR Audit Service, Internal Audit Division, OIOS

From: Kelly T. Clements, Deputy High Commissioner 

File Code: FIN 2.12

Subject: **Response to the draft management advisory on the implementation of the Enterprise Risk Management Framework at UNHCR (Assignment No. VR2017/160/02)**

Date: 27 October 2017

1. Reference is made to the above-mentioned draft management advisory and the subsequent revision shared with the Chief Risk Officer on 26 October 2017, containing refinements of your views on the topic of risk tolerance and appetite (para 16.). We have no further comments.

2. On behalf of the High Commissioner I would like to thank OIOS for the draft advisory which provides useful observations and suggestions to improve risk management in the organization. Your feedback will contribute and inform the planned revision of the Enterprise Risk Management framework after the updated international standard ISO 31000 is issued.

Thank you.

---

CC: **HC00**: Grandi, Okoth-Obbo, Türk, Lombardo, Madjora; **IG00**: Färkas; **CM00**: Daly; **DH99**: Harutyunyan

Mr. Martin Howarth, Auditing Assistant, UNHCR Audit Service, Internal Audit Division, OIOS  
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS