



## OFFICE OF THE INSPECTOR GENERAL

### Assessment of the FAO Risk Management Practices (AUD0223)

#### EXECUTIVE SUMMARY

The Office of the Inspector General (OIG) conducted an assessment of FAO's risk management maturity level benchmarked to the Reference Maturity Model for Risk Management <sup>1</sup> approved by the United Nations High-Level Committee for Management (HLCM). The assessment was carried out between February and September 2022 and focused on FAO's risk management practices in 2021 and 2022.

The Reference Maturity Model defines five levels of risk maturity for enterprise-wide risk management as shown in the table below.

Maturity levels	
Initial	Unstructured, managed informally/inconsistently, ad hoc, reactive.
Developing	Structured implementation, basic architecture, some reporting and repeatable management processes.
Established	Defined/documentated and standardized processes, good organizational coverage, some evidence of use and embedding. Regular reporting and escalation, information used in operational decision-making.
Advanced	Well structured, strong evidence of embedding. Standardized reporting and thresholds for escalation and management action. Information used in strategic decision-making.
Leading	Fully embedded. Escalation mechanisms well understood and used at all levels of the organization. Innovative/creative approach delivers continuous improvement and is able to adapt as the organization changes.

#### Objectives

The assignment had two main objectives:

- To determine the current maturity level of FAO's risk management practices based on the Reference Maturity Model (Objective 1); and
- To provide recommendations for improvement to FAO's risk management practices (Objective 2).

#### Main observations and conclusions

OIG assessed that FAO is, overall, at a **Developing** level of risk management maturity as measured by the Reference Maturity Model. The Office of Strategy, Programme and Budget (OSP) reached the same conclusion in a self-assessment of the model in 2021. The basic architecture of a risk management system is in place and the Enterprise Risk Management (ERM) Team of OSP has successfully implemented a system and process to complete risk logs across the Organization with the support of an established network of risk focal points. Overall, risk awareness among managers and personnel has improved in the Organization in recent years.

The Organization has reached an Established level of maturity in terms of its risk management governance and organizational structure and risk management systems and tools, while it is at a Developing level regarding the other four dimensions assessed. The results of OIG's assessment in each of the risk management dimensions (Objective 1) and the key actions required to advance to higher levels of risk management maturity (Objective 2) are shown in the table below.

<sup>1</sup> [Reference Maturity Model for Risk Management](#)

Areas	Maturity Levels				
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Enterprise Risk Management (ERM) Framework and Policy	Guidelines are in place to complete risk logs across the Organization. The Risk Management Policy is incomplete and outdated. Risk appetite and/or tolerance have not been established.				An updated risk policy and strategy are needed to integrate and coordinate risk taking across the Organization. The Organization's risk appetite should be established to guide risk taking. FAO's desired risk maturity level needs to be determined.
Governance and organizational structure	The coordination role for risk management is assigned to the ERM Team within OSP. The Core Leadership Team has assumed the role of a Risk Committee but it has met only twice and is yet to become fully functional.				Responsibility for risk management, including for risk owners, the ERM Team and second line of management, needs to be clearly articulated. Governance reporting on risk should be defined for the Oversight Advisory Committee and FAO Governing Bodies. FAO could consider the benefits of assigning responsibilities for coordinating the corporate risk management process in the Organization to a full time ERM Team leader supported by an adequately resourced team.
Process and integration	A process is in place to capture information in risk logs across FAO operations, but it is not adequately integrated with implementation of the internal control framework or sufficiently linked to the planning process.				Risk guidance for systematic risk assessment, response, monitoring, escalation and reporting needs to be improved. Better links need to be made between risk and internal controls, and risk management needs to be better integrated into results-based planning processes. A quality control process should be implemented for risk logs and to support the regular updating of the corporate risk log.
Systems and tools	FAO has risk logs in PIREs, <sup>2</sup> a system also used for budgetary and results-based monitoring. Fraud risk information is separately recorded in Fraud Prevention Plans filed on an electronic platform.				Better use of technology is required to integrate data across operations (including headquarters, field, programme, projects) and to provide functionality for risk analysis and reporting.
Risk capability	Support for risk capabilities has focused on providing training and guidance for completing risk logs. Risk analysis and reporting are limited.				Support for risk management competencies needs to be enhanced and training programmes developed accordingly for Senior Management and other staff with risk responsibilities. Timely, accurate risk management information reports are required to support decision-making.
Risk culture	The culture at FAO is perceived to be mainly risk averse. The current control environment does not encourage innovation and smart risk taking.				Senior Management should clearly communicate expectations; systematically demonstrate a commitment to risk management; and implement mechanisms to ensure appropriate risk taking is supported, rewarded and assessed in personnel performance management.

The key underlying causes that impeded the Organization from advancing to the next level of the Reference Maturity Model were:

- **Enterprise Risk Management Framework and Policy:** FAO did not update its risk management policy due to competing priorities, resource constraints and pandemic-related delays.
- **Governance and organizational structure:** The Core Leadership Team assumed the function of a Risk Committee in February 2022 but it has not yet become fully functional in directing risk management responsibilities in the Organization. FAO also does not have a dedicated Chief Risk Officer, although the Director, OSP is de facto performing the function on a part-time basis. Similarly, the ERM Team is led by a P-5 Senior Strategy and Planning Officer on a part time basis. The team has only three full-time staff.

<sup>2</sup> PIREs: Programme Planning Implementation Reporting and Evaluation Support System.

- **Process and integration:** With its limited resources, the ERM Team decided to take a phased approach to implement risk management processes. The team developed risk log processes, implemented internal controls reporting and made improvements to the fraud prevention plans; however, without well-defined linkages to integrate the results from these processes in planning and implementing internal control systems.
- **Systems and tools:** The systems for risk management are not integrated and have limited data analysis and reporting functionality. There are also no automated alerts for pending actions.
- **Risk capabilities:** Given its limited resources, the ERM Team did not prioritize the provision of risk management training for the Core Leadership Team and other FAO senior managers. The Core Leadership Team acting as the Risk Committee has yet to define and agree with the ERM Team the requirements for corporate reporting of risk information across the Organization, reporting to the Core Leadership Team as well as reporting to the Oversight Advisory Committee and FAO Governing Bodies.
- **Risk culture:** Generally, FAO's culture is perceived as "risk averse". Several interviewees lamented the large amount of control and bureaucracy, which they perceived as having been designed to limit errors and avoid damage to the Organization's reputation and which inhibited risk-taking. The one-year contract terms for Directors and other personnel also reduce the willingness to take risks due to the perception that there is not enough time to fix mistakes or change course before contract renewals.

Although the HLCM Reference Maturity Model for Risk Management was not intended to be used for compliance purposes, and FAO Senior Management should choose its targeted maturity level in consultation with Member States, enterprise-wide risk management, when implemented in the right way, is an essential enabler of the Organization's success. At the moment, FAO does not have a complete and accurate picture of its risk landscape and the effectiveness of the actions taken to manage key risks across the Organization. In May 2022, the ERM Team prepared a draft Risk Management Action Plan for 2022 to 2024 to reach the Established level of maturity. To support the ERM Team in implementing it, the Organization needs to further invest resources in and provide strong managerial commitment to risk management.

Therefore, OIG is of the opinion that **Major Improvement is Needed** in the Organization's risk management practices, as reflected by the actions required to be taken, before it can be assessed to have reached at least an Established level of maturity in each of the six dimensions of the Reference Maturity Model.

#### Agreed actions

This report contains six actions that the Core Leadership Team and the ERM Team have agreed to undertake. They are committed to fully implement all actions by December 2024. The high priority ones relate to: (i) determination of the Organization's desired end-state risk management maturity level and a road map for achieving it; (ii) establishment of a governance structure for risk management with clear roles and responsibilities for the Core Leadership Team, the Director of OSP, ERM Team, and risk owners, and criteria for risk-based delegation; (iii) development of managers' and key personnel's competencies in risk management and clarification of reporting requirements on risk information; and (iv) measures to support and reward appropriate risk-taking behaviour within the limits of the Organization's defined risk appetite.

*Mika Tapio*  
Inspector General

08 February 2023

## ANNEX: DEFINITION OF AUDIT TERMS

### AUDIT RATINGS

An audit rating system (defined below) has been used to rank the adequacy of internal controls <sup>3</sup> in each area.	
<b>Satisfactory</b>	The assessed controls, governance arrangements, and management of opportunities and risks, are adequate and effective to provide reasonable assurance that objectives are met.
<b>Some Improvement Needed</b>	A few specific weaknesses in the assessed controls, governance arrangements, and management of opportunities and risks were noted; generally however, they are adequate and effective to provide reasonable assurance that objectives are met.
<b>Major Improvement Needed</b>	Numerous specific weaknesses in the assessed controls, governance arrangements, and management of opportunities and risks were noted; they are unlikely to provide reasonable assurance that objectives are met.
<b>Unsatisfactory</b>	The assessed controls, governance arrangements, and management of opportunities and risks, are not adequate or effective to provide reasonable assurance that objectives are met.

<sup>3</sup> FAO's accountability policy, in an extension of the COSO internal control objectives, establishes five critical areas of performance relevant for assessing the adequacy of controls – effectiveness, economy and efficiency, compliance, reporting and protection.