United Nations Industrial Development Organization

Distr.: General
13 February 2025

Original: English

Industrial Development Board
Fifty-third session
Vienna, 30 June–3 July 2025

Programme and Budget Committee
Forty-first session
Vienna, 13–15 May 2025
Item 13 of the provisional agenda
General risk management

General risk management

Report by the Director General

In line with conclusion 2016/8 of the thirty-second session of the Committee, UNIDO continues to strengthen its enterprise risk management (ERM) framework and advance information security governance as essential components of its strategic operations. This work is also consistent with decision IDB.51/Dec.10 of the Industrial Development Board, which encouraged the Secretariat to finalize the process of re-establishing the ERM framework as a key element to address any risks which could prevent the delivery of mandates, as well as opportunities.

The present report provides an update to the documentation presented to the fortieth session of the Programme and Budget Committee and the fifty-second session of the Industrial Development Board on general risk management (IDB.52/9-PBC.40/9, IDB.52/33 and IDB.52/CRP.14), highlighting several key initiatives, including refining the Organization’s risk taxonomy to align with strategic priorities, establishing a robust governance structure to support risk management processes and enhancing information security governance to safeguard digital assets effectively. These efforts aim to improve risk identification and mitigation, support informed decision-making and ensure UNIDO’s resilience and alignment with its strategic objectives.

I. Introduction

1. This document provides an update to the documentation presented to the fortieth session of the Programme and Budget Committee and the fifty-second session of the Industrial Development Board on general risk management (IDB.52/9-PBC.40/9, IDB.52/33 and IDB.52/CRP.14), offering an overview of initiatives undertaken since the third quarter of 2024.

2. Previous reports by the Director General have tracked progress on the reference maturity model for enterprise risk management (ERM) as a United Nations-specific

framework and a benchmark for the risk management strategy of UNIDO. The aim of achieving an “advanced level” in the medium term is identified as a realistic target.

3. Since the last report, UNIDO bolstered its commitment to aligning risk management with strategic objectives and programmatic activities by integrating its risk profile with the proposal of the programme and budgets 2026–2027, making a pivotal step towards establishing a comprehensive, organization-wide risk management process deeply embedded with strategic planning and resource programming.

II. Strategic imperatives for institutionalizing enterprise risk management in UNIDO

4. With the promulgation of the adjusted UNIDO Secretariat Structure 2024 (DGB/2024/03), UNIDO established a dedicated unit, the Risk Management and Compliance Unit (COR/RCU), tasked with enhancing risk oversight, governance, cohesion and accountability by developing, coordinating and implementing UNIDO’s ERM and information security risk frameworks, as well as actively supporting senior management in fostering a robust risk culture. In addition to risk management and compliance, the Unit’s mandate includes a function related to cybersecurity.

5. Under the leadership of the ERM focal point, COR/RCU prioritized strategic engagement across directorates to enhance collaboration and alignment, completing various bilateral meetings with senior management on ERM progress, fostering its practical application. Notably, engagements conducted in the first quarter of 2024 were extended to include the new Directorate of Strategic Planning, Programming and Policy, created with the promulgation of the new Secretariat Structure 2024. The Unit also collaborated closely with organizational entities to contribute to the refinement of the UNIDO risk taxonomy and to reinforce its risk management support for the development of the medium-term programme framework 2026–2029 and the programme and budgets 2026–2027.

6. Regarding strategic alignment in ERM, COR/RCU finalized the ERM policy update, incorporating feedback from all directorates, with the remaining task being the alignment of the ERM framework with UNIDO’s governance framework. Key updates include aligning with the new organizational structure, setting clear risk management expectations, reinforcing the importance of tone at the top and defining specific roles and responsibilities across the Secretariat to embed a risk- and opportunity-aware culture into decision-making. The updated ERM policy also refines the risk appetite framework, defining processes and responsibilities for setting risk appetite; incorporates updated triggers for proactive risk identification during strategic planning, operational changes and programme and project implementation; strengthens the corporate risk register as a central tool for tracking and managing risks; and refines risk escalation and reporting pathways for the timely and effective mitigation of high and critical risks.

7. A proposed risk appetite statement has been developed and is under consideration by the UNIDO management. This document will provide a clear framework to guide the Leadership Board’s discussions and decision-making by setting clear expectations for risk management and the level and type of risk UNIDO is willing to accept in pursuit of its strategic objectives. It is crucial for aligning resource allocation with the Organization’s risk tolerance and supporting the achievement of UNIDO’s priorities by taking on appropriate risks with opportune and balanced mitigation measures. Once adopted, the statement can help strengthen UNIDO’s performance and safeguard its reputation and resources by improving the Organization’s ability to reduce the impact of critical risks, bringing greater consistency in risk-related decisions, promoting early detection of and response to risks, and ensuring accountability.

III. Enterprise risk management implementation at UNIDO

8. COR/RCU has performed multiple risk assessments, providing analyses of assumptions, risks and opportunities for key initiatives. These analyses mapped risks across various domains and will guide UNIDO in refining and mitigating risks as it pursues long-term goals.

9. A corporate risk register supported by a cloud-based risk management suite in Microsoft 365 Power Apps has been developed and is being piloted, automating risk assessment, escalation and reporting. This tool centralizes risk data, enhancing the efficiency, transparency and quality of risk assessments to support risk-informed decision-making. The full deployment of the app is scheduled for the first quarter of 2025.

10. Risks associated with implementing partner agreements remain a significant concern for UNIDO, often identified as a potential vulnerability within the Organization. Based on the Risk and Benefits Assessment of TC Project Implementation with Implementing Partner Agreements, COR/RCU comprehensively mapped implementing partners risks in alignment with the Organization's risk taxonomy and proposed risk owners and mitigation measures.

11. Regarding projects at risk, COR/RCU developed and shared a proposed risk classification for potential high-risk projects with all directorates. The risk classification scoring was reviewed to ensure alignment with the updated ERM policy. The classification aims to assist the Unit in its second line of defence role, providing oversight in the development and implementation of project risk management frameworks, as well as to support project managers and personnel as the first line of defence in identifying and prioritizing risks within their respective initiatives.

12. These activities reflect the Organization's ongoing commitment to advancing ERM maturity, as guided by the 2022 report of the External Auditor on UNIDO's risk management maturity assessment. The focus is on embedding ERM at the core of decision-making processes and within major strategic initiatives, ensuring its integration and practical application across both top-down and bottom-up information flows. This is supported by a more robust ERM governance, and enhanced risk identification, monitoring and reporting tools and capabilities, all of which are designed to strengthen the Organization's risk management framework.

IV. Cybersecurity framework and enhancements

13. UNIDO has made substantial progress in reinforcing its cybersecurity framework, implementing all pending recommendations by the External Auditor, as well as aligning with industry effective cybersecurity practices. Furthermore, a comprehensive overview of implemented measures related to UNIDO's cybersecurity framework has been presented in conference room paper IDB.52/CRP.14, as per the Joint Inspection Unit's recommendation contained in its report *Cybersecurity in the United Nations system organizations* (JIU/REP/2021/3). The Organization has established a solid cybersecurity governance framework by establishing the information security management system (aligned with the ISO 27001) through the UNIDO Information Security Policy (DGB/2023/01). In 2024, a new administrative instruction on the Information Security Risk Management Process (AI/2024/01) has been promulgated, describing the process to ensure that information security risks are identified, assessed, managed and mitigated effectively.

14. The dynamic nature of cybersecurity demands continuous vigilance, as challenges remain, mainly in the areas of implementing security by design, and enhancing the security monitoring and incident response processes. Addressing these challenges requires sustained focus, strategically balanced resource allocation and continuous improvement. Going forward, maintaining a proactive approach to cybersecurity will be essential for UNIDO. This includes regularly reassessing risks,

advancing technical capabilities and fostering a cybersecurity awareness culture across the Organization. These efforts will position UNIDO to withstand evolving cyber threats and protect its information assets, while also supporting its broader mission with resilience and confidence.

V. Action required of the Committee

15. The Committee may wish to take note of the information contained in the present document.