Organisation for Economic Co-operation and Development

C(2022)70/PART2/ADD4

For Official Use **English - Or. English**

2 December 2022

COUNCIL

Council

PERFORMANCE AUDIT: RISK MANAGEMENT SYSTEM AT THE OECD – EXECUTIVE SUMMARY OF EXTERNAL AUDITOR'S REPORT

JT03509217

Performance Audit: *Risk Management System at the OECD – Executive Summary of External Auditor's Report*

This audit was an update and follow-up to the assessment in the area of enterprise risk management (ERM) performed by the OECD Internal Audit (SGE/EVIA) in 2017. The objective of this performance audit was to evaluate the **effectiveness of the current Risk Management System** as defined in the OECD Risk Management Policy (RMP) both in terms of its design and implementation.

The audit focused on the design of the Risk Management System and evaluation of its particular elements by way of internal inquiries and questionnaire and external survey as well as sample checks of handling two critical risks and one non-critical risk.

The main criteria used in the audit were risk management standards (COSO, ISO 31000) and best practice generally accepted among international organisations (IOs).

The overarching opinion of the External Auditor is that the OECD has developed and implemented an effective Risk Management System (RMS) to identify and address risks, thereby enabling the Organisation to achieve its Strategic Objectives as presented in the Programme of Work and Budget (PWB). The External Auditor is of the view that the existing Risk Management System at the OECD is fit-for-purpose in accordance with the nature, size and complexity of the Organisation and the risks it faces.

The observations made during this performance audit, as well as the analysis of the results and findings of both external and internal audits conducted in the years 2019-2021, also indicate that the OECD's Risk Management System and practices provide reasonable assurance of safeguarding and protecting the Organisation's financial, human and physical resources.

That said, there is some room for improvement in some of the Organisation's risk management policies and procedures. The first area of improvement refers to better guidance for those involved in the risk management process, following the pattern adopted in the majority of other international organisations[1], which prepare two separate documents providing risk management guidance, a risk management policy and a risk management manual, the latter periodically updated.

In view of above, **the External Auditor recommended** splitting the current OECD Risk Management Policy into two documents: 1) a brief Risk Management Policy that outlines the purpose, scope, and principles of risk management, and 2) a longer manual that identifies roles and responsibilities as well as specifies how to exercise risk management in a more detailed form. The manual should be updated by the RSG, with the support of the Risk Coordination, in line with evolving needs, adopted best practices, as well as risk management standards (e.g. by adopting the IIA's 2020 Three Lines model and the "risk criteria" approach, and adaptation of the Risk Steering Group composition). Also, the existing risk management guidelines (e.g. document How to create a new risk? dated 2020) could be included in this manual. A policy and comprehensive manual will benefit and support all actors in the System and enhance all risk management activities.

The External Auditor observed that for cross-cutting risks, i.e. those that affect multiple organisational Strategic Objectives, Directorates, Divisions or other management units, the lack of a formal main (principal) risk owner may make it difficult to manage such risks

[1] Surveyed by the External Auditor during this audit.

centrally and address risk response across multiple units. Also, in the internal survey on RMS, particular risk owners and risk focal points commented that the situation is unclear in cases of cross-cutting risks, notably where the risk is co-owned by different Substantive Directorates, or by Substantive Directorates and Corporate Areas.

In view of above, **the External Auditor recommended** considering to identify one main (leading) risk owner for cross-cutting risks that should be managed by more than one Directorate. This would clarify the role and responsibility of the risk owner(s), and depending on the risk, it could be more effectively managed centrally. In addition, any response to the risks could be coordinated across multiple units by the main risk owner.

The External Auditor observed the crucial role of the Risk Coordination function in supporting the Risk Management System to ensure coherence and effectiveness of risk management processes and duties across the Organisation. The External Auditor drew attention to the fact that that the duties of persons exercising the function of Risk Coordination were performed on a part-time basis in addition to other tasks, without dedicated funding and specific IT support.

In view of above, **the External Auditor recommended** that consideration be given to more fulsomely resourcing the Risk Coordination function within EXD (by considering proposing additional dedicated budget, ensuring it is a primary time allocation for those staff assigned to the function, and by proposing resources for possible technical solutions). This would facilitate the performance of all the tasks associated with Risk Coordination, and raise awareness and understanding of risk management among the staff. This should also support the current responsibilities and potential work recommended in this report, in particular to: 1) create and develop the risk management manual and revised Risk Management Policy, 2) enhance risk communication and training to ensure consistency of response to risk across the Organisation, 3) support the risk owners in developing their own risk registers (sub-risk registers), 4) gather data and create effective risk communication material at various OECD levels in order to promote awareness of the general risk profile and cross-cutting risks and to assist in appropriate decision-making.

The External Auditor observed two intranet sites devoted to RMS. The one called OECD Risk and Crisis Management contained general information on the RMS, the Risk Register for Second Semester 2021, the list of risk owners and risk focal points, information on how to formulate and assess risk with the Risk Register template. The other one–Knowledge Centre-OECD Risk Management System–provided information not updated for more than two years.

In view of above, **the External Auditor recommended** that [one] intranet site be continued to be developed as an active and up-to-date information hub and as an education platform for all stakeholders. As such it would facilitate all the tasks of Risk Coordination as well as further raise awareness and understanding of risk management among the staff.

In order to look into the process of risk assessment and risk response, the External Auditor analysed two existing risks from the corporate Risk Register. First, the risk of damage or degradation of physical infrastructure (excluding IT), for which its risk assessment and risk response were considered as appropriate by the auditors.

Secondly, the External Auditor analysed procedures and their use in practice for the assessment and response to the risk of the *Loss of credibility for the Organisation due to inappropriate association with non-governmental entities*. The EA observed that the current risk criticality may be higher than actually assessed (as medium) and the risk response is not fully adequate with current external and internal situation. In connection

with this it was observed that reviews and evaluations of proposed grants is made by the Public Affairs and Communications Directorate (PAC), which is at the same time an active fundraiser and that the evaluation procedure was alleviated in 2020, which, in practical terms, allows a grant-receiving Directorate to make decisions on cooperation with a non-governmental entity even in cases of considerable uncertainty.

In view of the above, **the External Auditor recommended** the risk *Loss of credibility for the Organisation due to inappropriate association with non-governmental entities* be reassessed, and stronger risk responses (mitigation actions/procedures/measures) be designed to further reduce probability of "collaboration with inappropriate donors, sponsors or partners and/or cause a conflict of interests" as sources of this risk. In the case of PAC acting as an active fundraiser, the respective reviews for reputational risk should be done by an independent body or entity (e.g. OSG).

In the opinion of the External Auditor, the OECD RMS supports senior managers, who are entrusted with first line roles, to effectively manage the risks that may affect OECD Strategic Objectives. Furthermore, the second line provides sufficient complementary expertise, support, monitoring, and challenge. Finally, the Internal Audit is independent by way of its position in the Organisation and compliance of the OECD RMP with the IIA's Three Lines Model in relation to the Internal Audit function.

The External Auditor is also of the view that the Organisation reviews and improves its Risk Management System in a regular and consistent manner.

The benchmarking survey carried out among seven other international organisations, recognised as sharing with the OECD such features as size and nature of some of their operations, revealed that their risk management may be seen, at least partly, as comparable to the one of OECD's in terms of adopted standards and controlled processes. Differences lie in the treatment of cross-cutting risks, providing risk management guidance, and using risk management software.