Executive summary of the External Auditor's Report

Business Continuity Management at the Organisation for Economic Co-operation and Development

Proc. 25/D257/OECD

TRIBUNAL DE CONTAS

Objective

The objective of the performance audit was to assess whether the OECD's business continuity management system (BCMS) is fit for purpose.

Why does this matter

Business continuity focuses on maintaining operations at an acceptable level when normal processes are disrupted by unforeseen incidents or emergencies. An effective BCMS provides the necessary capabilities for the Organisation to recover essential processes and activities within agreed timelines and standards. Regular auditing of the OECD's BCMS is vital to ensure it remains capable of safeguarding the Organisation's resilience against potential threats.

General assessment

The OECD's current business continuity practices serve as a good foundation for further developments that could enhance effectiveness of the overall system. To support these improvements, specific recommendations have been made to guide future initiatives.

Key findings and recommendations

The Organisation's BCMS constitutes a good stepping stone upon which further developments can be made to enhance the resilience of the Organisation.

Until 2020, business continuity at the OECD was addressed through function-specific protocols, such as IT (Information and Technology) disaster recovery planning, contingency procedures for facilities, and security response protocols, each maintained by the responsible corporate function. In response to the COVID-19 pandemic, the Organisation formally consolidated these arrangements into an integrated Business Continuity Plan (BCP).

The BCP and the Crisis Management Plan (CMP) are the two main references concerning the OECD's BCMS. The BCP includes all centrally managed activities provided by the Executive Directorate (EXD). It is activated by the Executive Director in a situation of crisis and identifies the key personnel responsible for the resumption of each of the directorate's activities in the event of a disruption. Additionally, it sets time objectives for the resumption of these activities. However, several key elements of the OECD's BCMS, including the scope of the system and the delineation of responsibilities and authorities, are not explicitly documented. Instead, they rely, both directly and indirectly, on guidance inferred from various documents.

In view of the above findings, the External Auditor recommended that, based on the existing OECD's resilience framework, the BCMS of the OECD be outlined in a policy that: (1) facilitates communication within the Organisation; (2) establishes a solid framework for setting business continuity objectives and scope; (3) defines the authority, roles, and responsibilities of key stakeholders; and (4) allows for the evaluation and continual improvement of the system.

The BCP and the CMP are high-level documents, containing confidential information and shared on a need-to-know basis. Their concise nature and limited accessibility restrict Organisation-wide guidance and awareness. Regarding the responsibilities entrusted to the policy directorates in business continuity, enhancing the availability of information could support more effective management. Significantly, 14 of the 16 policy directorates reported either no participation in BCP activities or involvement only in indirectly related activities, such as IT and cybersecurity training, assessments, and inventories.

In view of the above findings, the External Auditor also recommended that the Organisation enhance managers and staff understanding of the BCMS of the OECD and the fundamental principles of business continuity through specific training and awareness sessions targeted at those directly involved in business continuity, as well as by increasing the availability of informational resources.

One of the key features of an effective BCMS is the assessment of relevant risks of disruption that could impact business continuity. The current Enterprise Risk Management framework of the OECD effectively supports the identification of risks and opportunities relevant to business continuity management. The business continuity management practices related to the most significant risks identified are those closest to meeting international best practices.

A crucial element of an effective BCMS is the existence of a Business Impact Analysis (BIA), which enables the identification and classification of activities that require business continuity solutions, as their disruption would result in unacceptable impacts on the Organisation. However, the BIAs conducted by the OECD in 2017 and 2023, which were exclusively focused on IT applications, were not intended to directly support the further development of the BCP or enhance business continuity practices at the directorate level. To further enhance the effectiveness of its BCMS, the OECD can benefit from a comprehensive BIA focused on the main types of policy outputs, modelled on ISO 22317:2021 (Security and resilience – Business continuity management systems – Guidelines for business impact analysis).

In view of the above findings, the External Auditor recommended that the Organisation conduct a comprehensive BIA for main types of policy outputs, as well as the activities and resources that support them, in order to enhance business continuity strategies and solutions.

The primary area of business continuity management within the scope of policy directorates responsibility is decentralised IT management. Most directorates claim to use mainly the centrally managed IT infrastructure of the OECD, although some also declared independently managing third party/cloud hosted applications. At the directorate level, excluding EXD, there are no business continuity plans, and when business continuity strategies and solutions do exist, they are not documented.

In view of the above findings, the External Auditor recommended that the information necessary to understand the roles, responsibilities, plans, decisions and activities of key stakeholders in the Organisation’s BCMS be comprehensively documented and regularly updated in accordance with international best practices.

Although the OECD conducts annual crisis management exercises, which can provide useful information for business continuity management, the Organisation lacks a dedicated exercise plan for business continuity strategies and solutions. The effectiveness of existing controls depends on specific practices, exercises, and tests conducted at the service level, but these activities are not tailored for comprehensive business continuity assessment. Although the effectiveness of the OECD's BCMS can be enhanced, the current system has already demonstrated its effectiveness in managing two disruptive events: the COVID-19 pandemic and the Paris 2024 Olympic Games.

Considering the aforementioned findings, the External Auditor recommended that the Organisation, drawing on its annual crisis management exercises, develop and implement a documented and coordinated exercise programme for the existing business continuity strategies and solutions, enabling the assessment of their effectiveness and supporting the continual improvement of its BCMS.