Organisation for Economic Co-operation and Development

C(2024)81/PART2/ADD6

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

4 November 2024

COUNCIL

Declassified

Council

2023 PERFORMANCE AUDIT: DECENTRALISATION – PHASE 2 – DIGITAL SECURITY AT DIRECTORATES' LEVEL

Executive Summary

JT03554609

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

NAJWYŻSZA IZBA KONTROLI
SUPREME AUDIT OFFICE OF POLAND

Executive Summary of the External Auditor's Report

DECENTRALISATION – PHASE 2 – DIGITAL SECURITY AT DIRECTORATES' LEVEL

1. The objective of this Performance Audit was to assess whether digital security was effectively protected under the Organisation's decentralised management, by checking whether relevant policies and control measures are consistently applied at Directorates' level and whether Directorates and other organisational units self-assess effectively their maturity in this area.

2. To make a broad and balanced assessment, the External Auditor took into account the results of his previous audits with relevance to the subject-matter of the current audit, such as Risk Management System at the OECD (audited in 2022) and Decentralisation of OECD – Phase 1 (audited in 2023).

3. Based on the results of the above-mentioned audits and performing additional audit procedures, the External Auditor decided to focus on the application of digital security Policies, Guidelines and Operational Documentation in decentralised substantive Directorates, the impact of software acquisition by these Directorates on the Organisation's IT security, and Self-Assessment exercise of their digital security maturity.

4. To achieve the overall objective of the audit, the work mainly comprised examination of relevant Policies, Guidelines and Operational Documentation, analysis of the reported IT applications, inquiries with the staff responsible for ensuring digital security in Directorates and sample checks of chosen IT solutions. The main area of the External Auditor's interest was whether Directorates carried out risk assessment of used applications in consultation with EXD/DKI, as these are captured by the digital security policy framework of the Organisation. The External Auditor also reviewed Self-Assessments for 2023 of all Directorates.

General assessment

5. **The OECD recent initiatives in the field of digital security positively contribute to its increase at the level of Directorates and other organisational units. Digital products and services, including cloud services, are subject to a risk assessment in order to avoid the use of IT solutions that may pose a threat to the Organisation. The introduced Self-Assessment exercise generally enables for parties concerned to make a detailed analysis of various aspects of digital security to be achieved by decentralised Directorates.**

6. **The Policies, Guidelines and Operational Documentation implemented along with the Self-Assessments exercise, if their potential is fully exploited, create some capacity for the IT digital security to be monitored, problems to be revealed and solved, and improvements if needed to be made, thus providing useful tools, among a broader toolkit, to support the management of risks in respect of digital security in the decentralised Organisation.**

7. **The analysed newly acquired applications were selected in line with substantiated needs, accepted in due process and they were in scope to be subject to a risk assessment before they were deployed and while they continued to be used. The examined contractual arrangements included security clauses. This shows that the relevant control measures were applied and monitored.**

8. However, the External Auditor has found several deficiencies, which may potentially increase the risks to digital security at Directorates level if not remedied. That is why some adjustments are needed to address deficiencies in performing risk assessment for cloud services as well as the processing of digital security Self-Assessments.

9. Although all of the IT software used in Directorates shall be subject to the risk assessment, in practice it was not always made for the cloud-services. It was found during the audit that three out of five examined Directorates and other organisational units did not

submit Digital Security Risk Assessment requests prior to the deployment of eight (out of 16 audited) cloud services, though they were required to do so in compliance with the OECD Information Technology Policy Security in Project Design and Build and the OECD Cloud Policy.

10. In connection with this, it is recommended to **continue increasing digital security awareness among the staff and management in respect of Directorates' compliance with the Digital Solution Risk Assessment procedure, the Cloud Usage Request Assessment Procedure and the new security measures for the acquired IT solutions that are deployed outside the OECD network and/or premises.**

11. Although the results of the Self-Assessment exercise were reported to the executive management[1], executive management had insufficient knowledge whether Directorates undertook relevant corrective actions when the set targets were not achieved. Under the current procedures, Directorates are encouraged but not obligated by statute to provide comments or action plans in this regard to the executive management. As a consequence, information about deficiencies and proposed actions for digital security improvement provided in Self-Assessments and sent to the executive management were not complete.

12. In connection with this, **it is recommended that the OECD Information Technology Guideline OECD Digital Security Assertion include the responsibility of Directorates and other organisational units to present -when the expected level of maturity has not been achieved- relevant action plans with measures to correct deficiencies.**

13. All Directorates prepared Self-Assessments for 2023 showing their maturity level in the context of digital security. However, one Self-Assessment was not submitted to the Office of the Secretary-General. It was filled in by an organisational unit hosted within the Development Co-operation Directorate and has not been included in the Self-Assessment submitted by this Directorate.

14. In connection with this, **it was recommended to ensure that all Self-Assessments prepared by organisational units are submitted to the executive management**.

15. There was also an inconsistency in the Self-Assessments instructions regarding the target level of identification of sensitive information and the level of its protection. Specifically, the target level for the identification was set lower than the target for the protection of sensitive information, which may pose problems for the Directorates to interpret them properly.

16. In connection with this, **it was recommended to consider setting the target of statement 7 *(Sensitive information, including personal data, managed by the Directorate/ Service/Programme has been identified)* at a level not lower than the target of statement 8 *(Sensitive information, including personal data, managed by the Directorate/Service/Programme has appropriate security measures applied)***.

[1] EXD and SGE.