

MANAGEMENT BOARD DECISION

DECISION No MB/2024/07

OF THE ENISA MANAGEMENT BOARD

of 6 June 2024,

on its opinion on final accounts for the financial year 2023

THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Having regard to:

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), in particular Article 31(5);
- Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council, in particular Article 102 (3);
- the draft audit report of the European Court of Auditors on the 2023 annual accounts of the European Union Agency for Cybersecurity received by the Chair of the Management Board and by the Executive Director of ENISA on 24 May 2024;

Whereas:

- (1) On receipt of the Court of Auditors' preliminary observations on the Agency's Provisional Annual Accounts, the Accounting Officer shall draw up the Agency's Final Annual Accounts and the Executive Director shall forward them to the Management Board for an opinion.
- (2) The Management Board shall deliver an opinion on the Agency's Final Annual Accounts.
- (3) By 1 July 2024, the Accounting Officer shall send the Final Annual Accounts 2023, together with the opinion of the Management Board, to the European Parliament, the Council, the Commission and the Court of Auditors.

HAS DECIDED TO GIVE THE FOLLOWING OPINION:

On the basis of the examination of the final accounts, the Management Board of the European Union Agency for Cybersecurity

1. Considers that sufficient assurances exist to conclude that the accounts for the financial year 2023 present a true and fair view of the Agency's overall financial position as reflected on 31 December 2023 and properly reflect the implementation of the Agency's budget for the year 2023.
2. Notes that the annual accounts of the Agency were verified by an independent external auditor as provided in the Financial Regulation, and that the European Court of Auditors considered the verification results when preparing its own final audit opinion, as stipulated in Article 70(6) of the EU Financial Regulation.
3. Notes the following preliminary observations raised by the Court of Auditors in its draft audit report on the 2023 annual accounts of the European Union Agency for Cybersecurity:
 - a) The operational payments made in the context of the "enhanced cybersecurity support from ENISA in the wake of Russia's invasion of Ukraine" are assessed as irregular whereas the specific contracts signed in 2022 do not provide sufficient details (quantities, date of deliveries) of the services acquired. Given the materiality of the transactions (EUR 13,2 million), the ECA may therefore qualify their audit opinion on the legality and regularity of the payments underlying the 2023 annual accounts of ENISA.
 - b) The MB Decision 2023/08 on derogating Financial Rules for the provision of the support to Member States to further mitigate the risks of large-scale cybersecurity incidents in the context of the emergency situation due to possible spill-over effect from the Ukraine/Russia conflict is deemed invalid by the ECA.
 - c) The usage of non-staff for the initiation of financial transactions does not comply with EU financial rules.
 - d) An unusual high rate of late payments.
 - e) A potential conflict of interest combining the roles of Accounting Officer and Internal Controls Coordinator.
 - f) Other weaknesses in the procurement procedures.
4. Notes that by applying *stricto sensu* the legal rules as per the ECA audit observations would have led to the non-execution of the "enhanced cybersecurity support" for Member States, and if the legal commitment would have taken place in 2023 (which is prohibited by the ENISA's financial rules when using 2022 budget), the funds would have been used for the same purpose, i.e. the same contractors would have provided the same services to the same beneficiaries.
5. Notes that ENISA has already addressed some of the identified weaknesses (incidents here above: a) and b) by using a fit for purpose legal instrument, i.e. a contribution agreement and d) and f) by implementing specific internal processes) and that ENISA is planning to set up corrective measures for the remaining ones (incidents c) and e) here above). In particular and most importantly, the successor of the "enhanced cybersecurity support from ENISA in the wake of Russia's invasion of Ukraine", the "Preparedness and Incident Response Support for Key Sectors' action" under the Digital Europe Programme has taken the legal form of a contribution agreement (for a total maximum cost of EUR 20 million) signed in December 2023 between DG CNECT and ENISA. Such Agreement with a maximum implementation period of 3 years allows the much-required operational flexibility to efficiently provide enhanced cybersecurity support for Member States in need.

Done in Athens, 6 June 2024

On behalf of the Management Board,
[signed]

Ms Fabienne Tegeler
Chair of the Management Board of ENISA