



REPLIES OF THE EUROPEAN CYBERSECURITY COMPETENCE CENTRE (ECCC)

TO THE EUROPEAN COURT OF
AUDITORS' SPECIAL REPORT
on "Detecting and responding to
cybersecurity incidents - EU
cooperation framework progressing,
but only partially effective due to
implementation delays and limited
information sharing"



Contents

I. THE ECCC REPLIES IN BRIEF	3
II. REPLIES TO THE RECOMMENDATIONS	3
RECOMMENDATION 4	3
RECOMMENDATION 5	3

This document presents the replies of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) to observations of a Special Report of the European Court of Auditors, in line with Article 265 of the [Financial Regulation](#) and to be published together with the Special Report.

I. THE ECCC REPLIES IN BRIEF

The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) takes note of the ECA's draft Special report on "Detecting and responding to cybersecurity incidents - EU cooperation framework progressing, but only partially effective due to implementation delays and limited information sharing" and would like to thank ECA for the professional and collaborative way in which the audit was conducted.

The ECCC also acknowledges and accepts the two recommendations addressed at the Centre and their potential to contribute to the improvement of the implementation of the Digital Europe Programme.

The ECCC would like to thank once again ECA and to assure it of our full cooperation in the implementation of the conclusions of this report, but also with the occasion of future audits.

II. REPLIES TO THE RECOMMENDATIONS

Recommendation 4

Ensure a robust ownership and control assessment of entities receiving EU funding under the Digital Europe Programme

The European Cybersecurity Competence Centre should:

- (a) obtain reasonable assurance that beneficiaries responsible for providing financial support to third parties have the administrative and technical capacity necessary to perform adequate ownership and control assessments, based on the existing methodology available to beneficiaries implementing financial support to third parties; and
- (b) check, on a sample basis, whether only eligible entities have received EU funding.

Target implementation date: (a) 2026, (b) 2027

The ECCC accepts recommendations 4.a) and 4.b).

Recommendation 5

Strengthen the performance monitoring framework of the cybersecurity component of the Digital Europe Programme

To enable adequate progress and performance monitoring, the European Cybersecurity Competence Centre should:

(a) ensure, prior to grant signature, that all projects have defined milestones, deliverables, and performance indicators that comply with the instructions provided in the application form;

(b) design and implement a robust system for the collection, traceability, verification, and aggregation of the data for the performance indicators of the cybersecurity component of the Digital Europe Programme, to ensure the indicators accurately reflect the results achieved.

Target implementation date: 2027

The ECCC accepts recommendation 5.a).

For the Digital Europe Programme, the ECCC will, to the extent possible and within the applicable regulatory framework, further strengthen the definition and consistency of milestones, deliverables, and performance indicators during the Grant Agreement Preparation (GAP). This includes reinforcing internal guidance and quality checks to ensure alignment with the requirements set out in the application forms.

The ECCC accepts recommendation 5b).

The ECCC notes that, for the Digital Europe Programme, it will work towards improving the collection, traceability, verification, and aggregation of performance indicator data, including through enhanced internal processes and guidance to beneficiaries, taking into account the corporate guidance on ensuring reliability of data that should be taken into account in defining any improved internal processes.