European Commission

Annual Activity Report 2025

Annexes

Directorate-General for Digital Services

Contents

ANNEX 1: Statement of the Director in charge of Risk Management and Internal Control

I declare that in accordance with the Commission's communication on the internal control framework ([1]), *I have reported my advice and recommendations on the overall state of internal control in the DG to the Director-General.*

I hereby certify that the information provided in the present annual activity report and in its annexes is, to the best of my knowledge, accurate and complete.

Brussels, 31 March 2026

(signed)

Natalia Aristimuño Pérez

([1]) C(2017)2373 of 19.04.2017.

ANNEX 2: Performance tables

This section is structured as follows:

General Objectives are the political objectives of the European Commission for the term 2025-2029, as defined in the Commission's strategic plan 2025-2029 ([2]).

Under each general objective, there are one or multiple specific objectives. DIGIT established these specific objectives in 2025, and they describe DIGIT's contribution to selected (Commission-wide) general objectives: DIGIT identified that it can contribute to the general objective 8, and to this end specified its own specific objectives (numbered 8.1, 8.2, 8.3, and 8.4). Equally, DIGIT contributes to general objective 1 (through its specific objectives 1.1 and 1.2) and to general objective 6 (through its specific objective 6.1) ([3]).

Under each specific objective there are:

- One or more **result indicators** These indicators measure and monitor DIGIT's progress towards the respective objective throughout the current Commission term (2025-2029).
- One or more **main outputs in 2025**. These are DIGIT's short-tern (annual) deliverables, and they were specified in the DIGIT Management Plan 2025 ([4]).

([2]) Commission Priorities 2024-2029 and Commission Strategic plan 2025-2029
([3]) DIGIT's Specific Objectives are defined in DIGIT Management Plan 2025, Part 1 Section 2.
([4]) DIGIT Management Plan 2025

General objective 8: A modern, high-performing and sustainable European Commission

Specific Objective 8.1: DIGIT facilitates and enhances digital sovereignty within the Commission IT

Related to spending programme(s): n.a.

Result indicator 8.1.1: Progress on the implementation of the actions identified in the DIGIT analysis for digital sovereignty

Explanation: As of early 2025, DIGIT is analysing the case for increased digital sovereignty across the Commission's IT activities and will propose pertinent actions. The indicator measures how many of the actions planned for 2025-2029 are completed, in % of the total number of 2025-2029 actions.

Source of data: DIGIT DDG/R.1

This result indicator is selected as a KPI

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
0%	30%	100%	0% In November 2025 the ITCB endorsed a digital sovereignty Action Plan, developed by DIGIT. DIGIT immediately started implementing the actions, and at end of 2025 multiple actions are ongoing, with none completed yet.

Main outputs in 2025:

Other major outputs

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Address the DWP sovereignty gap by exploring different fallback solutions for various DWP services	Prototype for the Linux endpoint as a complementary solution. Explore fallback solutions for communication and collaboration tools	Q2 2026	Ongoing
On Prem GPU Infrastructure support for AI Workloads	24by7 service operational	End of 2025	Completed On-prem GPU infrastructure is in production, actively supporting AI workloads for the GPT@EC platform.

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Extension of the Private Cloud Service catalogue with an EU sovereign stack	Assessment of an EU sovereign cloud stack. First PoC established.	End of 2025	Postponed Execution of the PoC deferred to 2026 pending completion of the sovereign cloud call for tender, to ensure compliance with tender rules.
Implement a Cloud Sovereign Region	Award a competition under Cloud DPS III to implement a Cloud Sovereign Region	End of 2025	Ongoing Competition has been published end 2025 and will be awarded by end Q2 2026.
Adapt and develop the network and network security services: align with new needs of service delivery, digital workplace and cloud services, including the use of a digital sovereign stack and shift to extensive use of open-source solutions [shortened]	Enable new IT strategies by designing a blueprint to provide network and network-services. New open source technical stack in production for teleworking, Internet access and protection of applications services	End of 2025	Ongoing Blueprints have been developed for 70% of the pertinent services. For the remote access services (including teleworking), activities have been finalised. For internet access services, activities are ongoing to migrate all environments and to develop additional capabilities for these services for a smooth migration of all the use cases. For web-protection services, test/dev and acceptance environments have been migrated to the new platform based on open-source solutions. Development of additional capabilities to support the production environments are necessary before migration of the production environments.
Execute the Testa-EIRIS strategy for the design and implementation of in-sourced robust and flexible Pan-European network services	Procurement stages ready	End of 2025	Finalised The service specifications for the underlay services have been published

Specific Objective 8.2: The Commission is resilient to cybersecurity threats

Related to spending programme(s): n.a.

Result indicator 8.2.1: Cybersecurity maturity

Explanation: As of early 2025, DIGIT is developing a new cybersecurity maturity indicator. The indicator will be based on the Risk Maturity Quadrant (RMQ) and will conceptualise maturity as good performance in important cybersecurity processes. Performance will be assessed both at Department and Information System level. The maturity indicator will be a composite of 14 individual indicators, related to the management of compliance, the security nature of the information systems, implementation of recommendations, resolution of reported issues, incident management, vulnerability and patch management, IT security plans and cybersecurity culture. The composite indicator will be measured on a scale from 0 (lowest maturity) to 5 (highest maturity).

Source of data: DIGIT S.1

This result indicator is selected as a KPI

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
The indicator was planned to be defined and a baseline value to be established in 2025.	Increase by 0.5 above the baseline	Increase by 1 above the baseline	RMI (Risk and Maturity Indicator): 46/100 (The RMI is reported here pending the development of the new cybersecurity indicator, whose development is put on hold to be aligned with the interinstitutional maturity model to be developed and endorsed by the Interinstitutional Cybersecurity Board (IICB) in 2026.)

Result indicator 8.2.2: Cybersecurity culture Explanation: As of early 2025, DIGIT is developing a new cybersecurity culture indicator. The indicator will be a composite one, combining clicking rates, reporting rates, knowledge scores and training participation. The indicator is measured on a scale from 0 (lowest maturity) to 5 (highest maturity). Source of data: DIGIT S.1			
Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
The indicator was planned to be defined and a baseline value to be established in 2025.	Increase by 0.5 above the baseline	Increase by 1 above the baseline	CSA (CyberSecurity Awareness indicator): 52/100 (The CSA indicator is reported here pending the development of the new culture indicator, whose development is put on hold to be aligned with the interinstitutional maturity model to be developed and endorsed by the Interinstitutional Cybersecurity Board (IICB) in 2026.)
Result indicator 8.2.3: Cybersecurity capability Explanation: The indicator assesses the Cybersecurity Incident Management Maturity of the Commission against baseline levels defined by ENISA ([5]) (basic / intermediate / advanced). As the indicator is being used in the Commission for the first time, an initial assessment will be carried out in 2025, establishing a baseline. Source of data: DIGIT S.2			
Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
The baseline value assessed in 2025 is 'INTERMEDIATE'	Maturity Level: Advanced	Maintain Advanced Maturity Level, keeping pace with evolving threats and technology evolution	INTERMEDIATE

Main outputs in 2025:

Other major outputs

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
An IT security controls baseline for Artificial Intelligence systems is developed	Baseline document is approved by IMSB (or pertinent governance body)	End of 2025	Finalised The baseline is defined and currently in use.

([5]) ENISA (2022): ENISA CSIRT Maturity Framework - Updated and improved

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Six phishing exercises are launched within 2025 targeting all Commission staff	All six exercises are closed	End of 2025	Finalised Six phishing exercises successfully launched
Cybersecurity training and awareness content for Artificial Intelligence is developed	Training and awareness content for AI is available on Cybersecurity portal	End of 2025	Finalised A specific presentation on AI & Cybersecurity was created, as part of the Cybersecurity Training Programme, and will be provided to all Commission users through EULearn training offering.
The Local Informatics Security Officer's role is further reinforced, leveraging the LISO network and other available communities of security practitioners, for providing the LISOs with additional support, guidance and prioritisation	An Ares note clarifying the role of the LISO is sent to all DGs	End of 2025	Finalised An Ares note clarifying the role of the LISO is sent to all DGs
The mobile devices security programme is developed, and a governance model is established	The project charter is approved by DIGIT Senior Management	End of 2025	Finalised
A Cybersecurity Incident Management Maturity indicator baseline is established for the whole Commission, extending from ENISA's CSIRT Maturity Framework	The indicator is approved by DIGIT Management (Head of Unit)	End of 2025	Finalised

Specific Objective 8.3: DIGIT drives forward the digital transformation of the Commission, in terms of technologies, ways of working, and outputs (policies and legislative initiatives)

Related to spending programme(s): n.a.

Result indicator 8.3.1: Commission Digital Landscape maturity

Explanation: This indicator provides a snapshot of current state of Commission's digital landscape from the perspective of technical and strategic fit, thus showing the effectiveness of DIGIT's support to the corporate digital transformation. The maturity level is expressed on a scale from 0 (least mature) to 10 (most mature). The criteria to assess the maturity level are currently under evaluation and will be provided by end of 2025.

Source of data: DIGIT.A.1

This result indicator is selected as a KPI

Baseline (2024)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
A baseline value was foreseen to be available by end of 2025 and included in the 2025 Annual Activity Report.	Maturity level: increase compared to baseline	Maturity level: increase compared to interim milestone	The calculation of the baseline is postponed until the inclusion of a sovereignty indicator in the Digital Landscape cartography, as sovereignty will impact the fitness values. This initiative is part of DIGIT's ongoing sovereignty action plan and is expected to be completed by 2026.

Result indicator 8.3.2: Adoption of digital trust enablers

Explanation: This indicator measures the extent to which digital trust enablers are integrated and utilised within the European Commission's digital solutions. Digital trust enablers encompass a range of managed services that ensure secure, transparent, and reliable digital interactions. These may include identity and access verification systems (EU Login, EU Access, EU Verify, eID and in the future digital wallets), data integrity solutions (EU Send), digital signature and preservation services (EU Sign) and several others.

The measurement unit for this indicator is the percentage (%) of relevant digital solutions within the Commission that have successfully adopted one or more digital trust enablers. This percentage will be assessed against the total number of digital solutions as defined in the annual 'State of the Digital Commission' Report

Source of data: DIGIT B.3

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
Among the Commission's circa 1.000 operational digital solutions, 10% adopted digital trust enablers as Managed Service (excluding EU Login, which is mandatory). An additional estimated 3% adopted digital trust enablers as Building Block.	Increase by 5% compared to 2025 baseline	Increase by 5% compared to interim milestone	13% (established as baseline)

Result indicator 8.3.3: Percentage of legislative proposals with a Legislative Financial and Digital Statement (LFDS) identifying at least one requirement of digital relevance compared to the total number of legislative proposals with an LFDS

Explanation: The indicator measures the Commission's maturity to use digital thinking during policy design thus fostering administrative simplification and burden reduction. The indicator value is the absolute number of legislative proposals with an LFDS where DIGIT was consulted in the inter-service consultation, per calendar year.

Source of data: DIGIT B.2

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
18 (Baseline captured in the second half of 2025)	Increase by 15% compared to 2025 baseline	Increase by 25% compared to 2025 baseline	Increase by 69% (DIGIT was consulted on 42 files with an LFDS, out of which 29 contained at least one digital requirement)

Result indicator 8.3.4: Progress in rolling out the Cloudification programme at the scale of the European Commission

Explanation: The Cloudification programme accelerates the modernisation of mainly, but not only, existing Information Systems to reap the benefits of Cloud technology and concepts. The programme helps DGs migrate their Information Systems to a hybrid cloud environment, considering each DG's unique needs and IT maturity. The Cloudification programme complements and works closely with the Cloud Acceleration Programme (CAP), which can provide the tooling for moving information systems to the cloud. The indicator measures the number of Information Systems being analysed by the Cloudification Programme team.

Source of data: DIGIT B.4

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
20% of the existing Information Systems have a high-level review analysis being performed.	50% of the existing Information Systems have a high-level review analysis being performed.	90% of the existing Information Systems have a high-level review analysis being performed.	Baseline value reached

Result indicator 8.3.5: Use of the Commission's corporate general-purpose generative AI solution

Explanation: The indicator measures the use of GPT@EC, offered by DIGIT at corporate level to improve the efficiency and effectiveness of Commission staff tasks. The indicator value is calculated as the percentage of returning users per month (latest available monthly value).

Source of data: DIGIT B.1

Baseline (2024)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
20% (October 2024)	30%	40%	35%

Main outputs in 2025:			
Other major outputs			
Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Release the API access to GPT@EC Pilot Large Language Models (LLMs)	Fully migrate GPT@JRC API users to GPT@EC and onboard all new requests received in 2025	End of 2025	Finalised GPT@JRC API users have been migrated to GPT@EC and the onboarding of all new requests received in 2025 has been realised.
State of the Digital Commission Report 2024 (SOtDCR)	Adoption of Report by ITCB	Adoption of report by ITCB in Q2 2025	Finalised Report presented in Information Technology and Cybersecurity Board (ITCB) on 28/04/2025 and to Corporate Management Board (CMB) on 14/5/2025.
Rollout of High Frequency Procurement for the Professional Services Broker	Number of use cases covered by HFP: Two in 2025	End of 2025	Ongoing A total of 17 contracts have been signed and/or are in the process of being awarded by end 2025, while another 22 are ongoing. Those contracts belong to three main use cases: DevOps, Activity-Based, and Time and Means.
Rollout of Software Broker	Launch the first competition implementing the brokering principles for SW acquisitions and including provisions catering for the Sovereign dimension for SaaS	End of 2025	Ongoing Timing of a new competition has been deemed premature by the management, focus, instead, was ensuring continuity and a phased approach, with an accent on a) securing new corporate agreements with critical providers such as Oracle and SAP (for which a brokering model has been implemented); b) improving the SIDEIII delivery, and c) drafting a new agreement model (PASS+) with software suppliers, to complement and eventually supersede negotiated ELA's as first milestone towards a Software Broker at scale. Such PASS+ also includes provisions for tackling the Sovereign dimension for SaaS, based on the Sovereign Framework of the Commission.

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Cloud Acceleration Programme (CAP). The Cloud Acceleration Programme provides tooling for DGs to move Information Systems to the cloud. It works closely with the Cloudification program, which provides DG-specific guidance and support.	Enable cloud adoption at scale at the European Commission by designing a blueprint for DIGIT to provide corporate cloud-based services.	End of 2025	Ongoing 1st year executed spent 3M€, supporting the deployment of the new generation of DIGIT managed services (Gen3) in public clouds.
Timely and accurate delivery in accordance with client agreements under the main solution provision partnerships (HRT, HAN, Decide, European Crisis Management Platform)	HRT wave 1 projects in production (Onboarding, Preselection, HR Service Desk); New Decide technical framework and PoC of main concepts; ECMP foundations setup	End of 2025	Finalised All IT workplans delivered on time and in accordance with client agreements.
Digital-ready policymaking (DRPM) guidance and training	Guidance and training resources are available for all main pillars of the DRPM framework on the DRPM support service hub	End of 2025	Finalised
DRPM tooling	Proof of Concept of AI-assisted completion of the digital dimensions chapter of the Legislative Financial and Digital Statement finalised	Q1 2025	Delayed Finalised in Q1 2026
EC Open Ecosystem Strategy	New open source strategy for European Commission	Q1 2026	Ongoing Initiative carried out in collaboration with CNECT. Proposal of DIGIT related actions endorsed by the ITCB in December 2025
code.europa.eu	code.europa.eu is migrated to a more resilient and sovereign infrastructure	End of 2025	Finalised Migration performed in September 2025

Specific Objective 8.4: Commission staff have at their disposal tools fit for a modern, resilient and collaborative administration

Related to spending programme(s): n.a.

Result indicator 8.4.1: User satisfaction with Digital Workplace (DWP)

Explanation: DIGIT annually surveys its user population for their satisfaction with DWP services. Users score their satisfaction with each individual service. The indicator is calculated as: number of individual scores of 'neutral' or higher, divided by the number of individual scores, multiplied by 100%.

The individual services included in the indicator are subject to change throughout the 2025-2029 period, depending on the evolution of the DWP service portfolio.

Source of data: Annual IT user survey / Digital Commission Dashboard (DIGIT C.5)

This result indicator is selected as a KPI

Baseline (2024)	Target (2029)	Latest known results (2025)
80% ([6])	At least 80% throughout 2025-2029	92%

Main outputs in 2025:

Other major outputs

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Prepare foundations for an AI-enabled Digital Workplace: complete tests and assessments for a data-driven, predictive Digital Workplace service	5 use-cases of major pain points analysed and tested in order to improve the quality and performance of the IT Helpdesk through data analytics and AI	End of 2025	Finalised 6 use cases analysed and assessed: 1. call duration insights, 2, automated ticked quality analysis, 3. knowledge gap detection, 4. laptop end of life replacement, 5. problem detection, 6, survey analysis/satisfaction tracking. The use cases are completed at the level of a Minimum Viable Product (MVP).

([6]) In the 2024 Annual Activity Report (AAR), the individual services included in the indicator are (a) PhishAlarm reporting button, (b) DWP portal, (c) Cybersecurity Portal, (d) AI@EC portal, (e) IT Knowledge Articles of the Staff Centre, (f) IT Helpdesk, (g.) IT section of the Staff Centre, (h) IT Hubs, (i) Private mobile device enrolment, (j) On the go, (k) EC Store, (l) DWP Settings, (m) EU Login Mobile App, (n) Easiness of the TPM set-up process.
The composition of the indicator is subject to change with the evolution of the DWP services (ITCB decision 09/2022). In 2024, the composite user satisfaction target was 80%, and DIGIT achieved 94% (AAR 2024).

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Extend the corporate Digital Workplace to Commission Representations in the Member States (33 Representations, by 2027)	10 Commission Representations covered for IT support within the corporate FWC	End of 2025	Finalised The major onboarding in terms of remote IT support, Welcome and DWP infrastructure (local server rooms consolidation) is completed. The remainder of the consolidation is linked to the telecom infrastructure and contracts and consolidating onsite IT support via managed service provisioning.
A resilient and secure Digital Workplace: - Migrate the non-DWP entities (JRC, COMREPs, OLAF) to Welcome - Migrate Digital Workplace Endpoints to Windows 11 - Migrate end-user Telephony from Skype to MS Teams - Phase out of NET1 Digital Workplace Services	- Migration is completed - 97% of Digital Workplace Endpoints are migrated to Windows 11 - Migration from Skype to MS Teams is completed - NET1 Digital Workplace services are phased out	End of 2025	Finalised NET1 services - phase out of some services has been completed (NET1 VPN / NET1 ITIC FARM) others are still ongoing (DFS) but on track. Overall the activity is considered closed.

General objective 1: **A new plan for Europe's sustainable prosperity and competitiveness**

Specific Objective 1.1: DIGIT facilitates public sector interoperability across the Union for a more competitive, faster and simpler Europe

Related to spending programme(s): Digital Europe Programme (DEP)

Result indicator 1.1.1: Number of solutions awarded the label 'Interoperable Europe' on the Interoperable Europe Portal

Explanation: This indicator reflects DIGIT's efforts in aggregating and showcasing diverse solutions aimed at enhancing public sector interoperability across Europe.

Source of data: DIGIT B.2 (Interoperable Europe Portal)

This result indicator is selected as a KPI

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
0	10	15	2

Result indicator 1.1.2: Number of training course certificates delivered by the Interoperable Europe Academy Explanation: Article 13 of the Interoperable Europe Act introduces the need to create learning materials on interoperability issues at Union level to enhance cooperation and foster the exchange of best practices between the staff of Union entities and public sector bodies, targeting public sector employees in particular at regional and local level. Upon completing an online learning course provided by the Academy and provided that they successfully pass a quiz at the end of the course, participants can obtain a certificate. This metric serves to quantify the outreach of the courses available in EU Academy. Source of data: DIGIT B.2			
Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
7328 (Baseline established at end of 2025)	Increase by 20% compared to 2025 baseline	Increase by 40% compared to 2025 baseline	7328
Result indicator 1.1.3: Number of interoperability assessment reports published on the Interoperable Europe Portal Explanation: Interoperability assessments are an instrument introduced by the Interoperable Europe Act to explore opportunities for enhancing cross-border interoperability of public services across the EU. The reports summarising the assessment must be published on a public website and shared with the Interoperable Europe Board thus allowing knowledge sharing on public sector interoperability. The Interoperable Europe Portal offers the possibility to perform or upload interoperability assessments and the indicator measures the total number of interoperability assessments published in this space. Source of data: DIGIT B.2			
Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
51 (Baseline established at end of 2025)	Increase by 15% compared to 2025 baseline	Increase by 25% compared to 2025 baseline	51

Result indicator 1.1.4: Number of federated open-source catalogues and open-source solutions Explanation: Number of federated open source catalogues: Total number of open source software catalogues managed by public administrations (at national, regional, or local level) that are successfully federated into the EU Open Source Solutions Catalogue. Units of measurement: Number of catalogues. Number of federated open source solutions: Total number of open source software solutions published in the EU Open Source Solutions Catalogue either via federated national, regional, or local catalogues, or individual onboarding (i.e. not linked to a specific catalogue). Unit of measurement: Number of solutions. Source of data: DIGIT B.2			
Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
6 catalogues 700 solutions	10 catalogues 900 solutions	12 catalogues 1000 solutions	9 catalogues 900 solutions

Main outputs in 2025:			
Other major outputs			
Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Stack of Digital Public Infrastructures: Adoption of reusable digital solutions by European Digital Public Infrastructures	- Digital Ecosystem reusing eDelivery: 2 additional ecosystems - Notification of the National Trust Lists by 100% of the EU/EEA Member States - Increase of the Trust Services offered by the EU Qualified Trust Service Providers (QTSPs) by 100% - Availability of the EU List of Trusted Lists (LOTL) >95%	End of 2025	Finalised Regarding Digital Ecosystems: In 2025, 4 additional ecosystems reuse eDelivery (European Maritime Single Window environment, electronic Freight Transport Infrastructure Exchange Environment, HealthData@EU Data Space, Digital Services Act - AGORA
Stack of Digital Public Infrastructures: Diversity of sectors implementing the reusable digital solutions	This is measured by monitoring the sectorial go-live of Once-Only in different sectors - Once-Only reuses most Building Blocks (eID, eDelivery and eSignature): 2 more sectors	End of 2025	Finalised - Lithuania and Finland live with procedures in the education domain - Italy went live in the field of regulated professions: Air traffic controller license and Student air traffic controller license

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Provision of reusable and interoperable digital solutions and building blocks	Continuous operation of the Building Blocks and eIDAS Dashboard websites: access points for information about the Building Blocks: 90% uptime	End of 2025	Ongoing
Implementation of the Interoperable Europe Act: Definition of the Interoperable Europe Agenda	Interoperable Europe Agenda published	End of 2025	Finalised Agenda adopted on 04/12/2025, available at Interoperable Europe Agenda
Implementation of the Interoperable Europe Act: Definition of the Interoperable Europe Monitoring and the first Annual Report on interoperability in the Union	Annual interoperability report published	End of 2025	Finalised First annual report adopted on 15/12/2025, First annual report on interoperability in the Union, COM/2025/860
Implementation of the Interoperable Europe Act: Regulatory sandboxes	Implementing act for the regulatory sandboxes adopted	Q2 2025	Finalised Implementing act published: Commission Implementing Regulation (EU) 2025/1420
Implementation of the Digital Europe Programme - Interoperability Chapter: Support to multi-country projects (MCPs) and cross-border initiatives for joint solutions development and cross-border data exchange	Calls launched	End of 2025	Ongoing The call was launched on 13/01/2026
EU Open Source Solutions Catalogue	EU Open Source Solutions Catalogue published	End of 2025	Finalised https://interoperable-europe.ec.europa.eu/eu-oss-catalogue
List of critical open source software used by public administrations ([7])	List published	End of 2025	Ongoing

([7]) As of 2025, DIGIT is carrying out a study to identify critical open source software. In the context of the study, critical open source software is defined preliminarily as any open source software that is crucial for a public administration or other essential public services. Such software, if it were to fail, malfunction, or become compromised, could severely impact operations or services.

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Execution of bug bounties to protect critical open source projects	Report published	End of 2025	Ongoing All bug bounty programmes started in Q4.2025 and will continue during 2026
Annual Progress Report on Implementation and Enforcement	DIGIT contribution provided to EVP report	Q4 2025	Completed

Specific Objective 1.2: DIGIT supports the uptake of AI and other digital innovation in European public administrations

Related to spending programme(s): Digital Europe Program (DEP)

Result indicator 1.2.1: Number of uses cases implementing AI or other emerging technology by public administrations in Europe

Explanation: The indicator reflects technological innovation activity in the European public administrations. The indicator is measured as the number of use cases identified by Public Sector Tech Watch. Data is collected by DIGIT via surveys, research and studies.

Source of data: DIGIT B.2

This result indicator is selected as a KPI

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
2007 use cases (Baseline established at end of 2025)	Increase by 20% compared to baseline	Increase of 50% compared to baseline	2007 use cases

Main outputs in 2025:

Other major outputs

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Development of pilot projects through the GovTech Incubator	New pilots launched	End of 2025	Ongoing 3 pilots were developed under the SGA that closed in June 2025. 8 new pilots at initial phases (started in July 2025)
Development of a registry of use cases implementing AI and other emerging technology	Public Sector Tech Watch launched	End of 2025	Ongoing More than 2000 cases are online. The action continues. Few more cases to be added in 2026.

General Objective 6: A global Europe: Leveraging our power and partnerships

Specific Objective 6.1: DIGIT cooperates with strategic partners globally on digital government, public sector interoperability and infrastructure, including trust services

Related to spending programme(s): n.a.

Result indicator 6.1.1: Number of countries and international organisations where cooperation is established
Explanation: The international dimension is key to this KPI since aligning candidate countries' interoperability frameworks with the Interoperable Europe Act and the European Interoperability Framework ensures seamless cross-border digital services, supports pre-accession integration, and reinforces a cohesive European digital space - benefiting both EU Member States and future members.
Source of data: DIGIT B.2/B.3
This result indicator is selected as a KPI

Baseline (2025)	Interim milestone (2027)	Target (2029)	Latest known results (2025)
Consultation of candidate countries on interoperability matters	Alignment of the national interoperability frameworks from the candidate countries with the Interoperable Europe Act and the European Interoperability Framework	EFTA + candidate countries + UA + MD + Türkiye included in the Digital Public Administration Factsheets	Iceland, Norway, Liechtenstein, Ukraine, Moldova, Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia, Türkiye (Digital Public Administration factsheets - 2025)

Main outputs in 2025:

Other major outputs

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Annual digital public administration factsheets	Number of candidate countries included in the digital public administration factsheets	3 candidate countries by end of 2025	Finalised Published in November 2025, https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/news/publication-2025-digital-public-administration-factsheets

ANNEX 3: Draft annual accounts and financial reports

The Annual Activity Report Annex 3 offers a dynamic view of the European Commission draft annual accounts and financial reports results per Responsible Department/Executive Agency, in a modern dashboard, on a single website.

The Annual Activity Report Annex 3 is available to view in the designated SUMMA dashboard that is available at the following link:
https://dashboard.tech.ec.europa.eu/qs_digit_dashboard_mt/public/extensions/BUDG_Annex3/BUDG_Annex3.html

The accounting situation presented in the Balance Sheet and Statement of Financial Performance does not include the accruals and deferrals calculated centrally by the services of the Accounting Officer.

ANNEX 4: Financial scorecard

The transition in 2025 to the Commission's new accounting system, SUMMA, has required the adjustment to a new system and has impacted budget implementation tasks, processes and financial management activities, particularly during the first part of the year. This has required careful management to ensure the same data quality as in previous years. In some cases, this has resulted in lower performance for some standard financial indicators such as the timely payments.

The Financial Scorecard is available to view in the designated SUMMA dashboard that is available at the following link:
https://dashboard.tech.ec.europa.eu/qs_digit_dashboard_mt/public/extensions/BUDG_Annex4/BUDG_Annex4.html

ANNEX 5: Materiality criteria

DG DIGIT uses the corporate guidelines for determining materiality as regards legality and regularity. According to these guidelines, only material reservations can be used to qualify the annual declaration. In the analysis leading to the decision to issue a reservation or not, the following steps are followed:

a. Identifying a deficiency (e.g.: a significant weakness of the control systems, insufficient audit coverage, a critical issue outlined by the European Court of Auditors, the Internal Audit Service or the European Anti-Fraud Office);
b. Determining if the deficiency falls within the scope of the Authorising Officer by Delegation's declaration (it relates to the reasonable assurance concerning the use of resources, sound financial management or legality and regularity of underlying transactions);
c. Qualitative assessment: assessing if the deficiency is significant in qualitative terms. In order to perform the deficiency's qualitative assessment, the following four pillars need to be analysed:
    - the nature and scope of the deficiency,
    - the duration of the deficiency,
    - the existence of compensatory measures (mitigating controls which reduce the impact of the deficiency),
    - the existence of effective remedial actions to correct the deficiencies (action plans and financial corrections) which have had a measurable impact;
d. Quantitative assessment: a deficiency, which is significant from a qualitative perspective, must be quantified in terms of 'monetary value of the identified problem'/ 'amount considered at risk'. In line with the guidelines agreed centrally in the Commission, DG DIGIT applies the recommended threshold of 2% i.e. when the value of the transactions affected by the deficiency represents more than 2%.

Since 2019 ([8]), a 'de minimis' threshold for financial reservations has been introduced. Quantified annual activity report reservations related to residual error rates above the 2% materiality threshold are deemed not substantial for segments representing less than 5% of a DG's total payments and with a financial impact below EUR 5 million. In such cases, quantified reservations are no longer needed.

For deficiencies which are considered significant from a qualitative point of view, but their financial impact is lower than the 2% threshold, DG DIGIT takes into account the potential reputational consequences they may entail. A reservation would be made if such a reputational event were to occur and negatively impact the image of the Commission. Such a reservation would be based on the nature of the impact on reputation, the breadth of awareness of the event, and the duration of impact of the reservation. Sustained or medium-term negative perception from stakeholders with an impact on the ability of DG DIGIT to meet its key objectives would be considered for a reservation.

Digital EUROPE programme

For Digital Europe the general control objective is to ensure that the residual error rate, i.e. the level of errors which remain undetected and uncorrected, does not exceed 2%.

([8]) Agreement of the Corporate Management Board of 30/4/2019.

HaDEA implements the audit strategy for the grant part of the whole Digital Europe Programme, serving all granting authorities of the programme ([9]). The audit strategy for Digital Europe Programme was drafted in consultation with the Digital Europe stakeholders and adopted on 5 July 2024.

The population of the programme is determined by the costs declared and paid to the beneficiaries or affiliated entities through financial statements which are the basis for the calculation of the EU contribution. The harmonised System for Grant Management (SyGMa) is the data source for the audit population and audit selection is performed via Selection Module SELMOD (AUDEX).

Error rate calculation

Detected error rates

The interval sample delivers the Detected Error Rate (DER) per programme.

Calculation of the detected error rate ([10]):

$$\text{DER (\%)} = \frac{\text{Amount of detected errors (EC share of)}}{\text{Sampled amount (EC share of)}}$$

The amount of detected errors corresponds to the amount of ineligible expenditure that results in a financial adjustment. It is equal to: [the EC-share of] the costs claimed as initially accepted, after the ex ante controls (on the basis of which the audited payment was made), minus, [the EC-share of] the costs claimed as finally accepted, after the ex post control (audit).

The sampled amount must be used as a denominator to calculate the detected error rate ([11]).

In the performance of an audit, the sampling applied is to ascertain the risk of a material error in the financial statement of a beneficiary. For cost-efficiency reasons, it might be lower than the cost accepted by the Agency.

([9]) In accordance with Annex I of the Delegation act to HaDEA, Commission Decision C(2021)948 final – 12/02/2021.

([10]) AAR standing instructions, additional guidance on the calculation of error rates, the financial exposure as amount at risk, the materiality for a potential reservation and the impact on the AOD's declaration (2022 version), available on BUDGWeb.

([11]) The European Court of Auditors in its 2018 Annual Report and its review of the Commission's ex-post audits observed that for Horizon 2020 the Commission's methodology for calculating the Error Rate leads to an understatement of the Error Rate the extent of which cannot be quantified. As a result of further related guidance received by the central services for the AAR 2019, the predecessor's entities have adapted their methodology for the calculation of the Error Rate in line with the Court's observations. Previously, the detected Error Rate was calculated by considering the full value of an audited financial statement in the denominator. Therefore, the Detected Error Rate calculation is based on the sampled EU contribution as the denominator for a more conservative approach.

Residual error rate

Given that usually only a sample of the programme's payments made is subject to ex post audits, not all payments can be fully cleared from errors. In reality, the larger part of payments remains un-audited and thus un-corrected; hence probably still affected by errors of the magnitude of the detected error rate.

The estimated Residual Error per programme is calculated as follows:

Residual Error = Uncorrected Errors + (Total EU Contribution – Total Sampled Contribution) * DER

The Residual Error is then divided by Total EU Contribution to give the Residual Error Rate (RER) expressed as a percentage as follows:

$$\text{RER (\%)} = \frac{\text{Residual Error (EC share of)}}{\text{Total EU Contribution}}$$

The RER represents the estimated error rate that remains in the population after audit corrections are implemented.

Multi-annual Residual Error Rate

Residual Error Rates are calculated on a multi-annual basis to reflect the multi-annual nature of the programme and projects.

Although not derived by statistical parameters that can be extrapolated to the unaudited payment population with statistical confidence, the detected error rate and the residual error rate from the ex post audits are a key building block in the assurance building process.

ANNEX 6: Relevant Control System(s) for budget implementation (RCSs)

The segment related to Procurement and administrative expenditure also includes administrative expenses for salaries and/or missions, which are reported by the service responsible for the commitment, although the payments are executed by another service, notably the PMO and/or DG HR ([12]). The executing service implements the necessary technical-level controls and submits a declaration to DG DIGIT on the compliance of these payments with the principle of sound financial management, as well as their legality and regularity. These expenses are considered to present a low level of risk and are therefore subject to a flat rate of 0.5%, as corroborated by the control results of the executing services. More information on the implemented controls can be found in DG HR and PMO annual activity reports.

([12]) Type III co-delegation for which these expenses were reported by the service executing the payments until 2024.

Relevant Control System: Procurement and administrative expenditure			
Stage 1: Ex ante – Planning Main internal control objectives: • Effectiveness, efficiency and economy of procurement procedures • Compliance (legality and regularity)			
Main risks *It may happen* ***(again) that...***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
The needs are not well defined (operationally and economically) and the decision to procure was inappropriate to meet the operational objectives.	Publication of intended procurements.	100% of the open procedures are advertised in the OJEU.	Effectiveness: Number of projected procurement procedures cancelled. Benefits (qualitative): Better value for money, deterrent effects, efficiency gains, system improvements, compliance with regulatory provisions, no litigation. Efficiency: Average cost per procurement procedure. Economy (costs): Estimation of cost of staff involved and the related contract values.
	Validation by AO(S)D of the justification (economic, operational) for launching a procurement process.	100% of the forecast procurements.	
	DIGIT senior management is consulted or informed about the general orientation, objectives of the procurement and means.	All major (above 143 000 EUR) procurement procedures are discussed at or submitted to the attention of the DIGIT Procurement Board chaired by the Director-General.	
The best offers are not submitted due to the poor definition of the tender specifications.	Supervision and approval of specifications.	100% of the specifications are scrutinised.	Effectiveness: Number of procedures where only one or no offers were received. Benefits: Limit the risk of litigation, limit the risk of cancellation of a tender. Efficiency: Estimated average cost of a procurement procedure. Economy (costs): Estimation of cost of staff involved and the related contract values.
	All pending legal challenges are closely monitored.	100% of litigation cases monitored.	
	Publication of intended procurements.	100% of the open procedures are advertised in the OJEU.	
The most economically advantageous offer not being selected, due to a biased, inaccurate or **'unfair'** evaluation process.	Formal evaluation process: Opening committee and Evaluation committee for procedures above 143 000 EUR.	100% of the offers analysed.	Effectiveness: Numbers of 'valid' complaints or litigation cases filed. Benefits: Potential irregularities/ inefficiencies prevented. Avoid contracting with economic operators in exclusion situation. Amount of procurements successfully challenged during standstill period. Efficiency: Estimate average cost of procurement procedure. Economy (costs): Estimation of costs involved.
	Consultation of the DIGIT procurement Board and GAMA advisory body.	Random selection by the GAMA body.	
	Exclusion criteria evidence of the successful tenderers checked.	100% checked.	
	Standstill period, opportunity for unsuccessful tenderers to put forward their concerns on decision.	100% when conditions are fulfilled.	

<table>
<tr><th colspan="4">Relevant Control System: Procurement and administrative expenditure</th></tr>
<tr><td colspan="4">Stage 2: Ex ante - Financial transactions
Main internal control objectives:
• Ensuring that the implementation of the contract is in compliance with the signed contract</td></tr>
<tr><th>Main risks
It may happen
(again) that…</th><th>Mitigating controls</th><th>Coverage frequency and depth of controls</th><th>Possible Cost-effectiveness indicators (3Es)</th></tr>
<tr><td rowspan="3">The products / services / works foreseen are not, totally or partially, provided in accordance with the technical description and requirements foreseen in the contract and/or the amounts paid exceed that due in accordance with the applicable contractual and regulatory provisions.

Business discontinues because contractor fails to deliver.</td><td>Operational and financial checks in accordance with the financial circuits.</td><td>100% of the contracts (SCs) are controlled.</td><td rowspan="3"><u>Effectiveness:</u>
Number of suspended invoices.
Number of refused orders at Financial initiator, verificatory and Authorising Officer level.
<u>Efficiency:</u>
Time-to- pay.
Late interest payment and damages paid (by the Commission).
<u>Economy (costs):</u>
Estimation of cost of staff involved.</td></tr>
<tr><td>Operation authorisation by the AO(S)Ds.</td><td>100 % of financial transactions controlled ex ante (this includes: commitments and payments).</td></tr>
<tr><td>Management of sensitive functions.</td><td>Each year.</td></tr>
</table>

Relevant Control System: Procurement and administrative expenditure			
Stage 3: Ex post – Supervisory measures Main internal control objectives: • Ensuring that any weakness in the procedures (procurement and financial transactions) is detected and corrected			
Main risks *It may happen* ***(again) that…***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
An error or non-compliance with regulatory and contractual provisions, including technical specifications, or a fraud is not prevented, detected or corrected by ex ante control, prior to payment.	Supervisory desk review financial transactions & procurement procedures (ex post control).	Sample in line with ex post procedures in place (for financial transactions & procurement procedures).	Effectiveness: Amounts associated with errors detected (related to fraud, irregularities and error). In % over total checked. Number of system improvements made. Benefits: Amounts detected associated with fraud & error. Deterrents & systematic weaknesses corrected. Preventing unauthorized access to financial systems. Efficiency: Costs of the ex post controls and supervisory measures with respect to the 'benefits'. Average cost of an ex post control. Average cost of financial systems access rights control. Economy (costs): Estimation of cost of staff involved.
	Review of ex post results.	Any systemic problem in procurement procedures and in financial transaction procedures are reported and analysed.	
	Review of exceptions and non-compliance reports.	At least once a year: Evaluation of non-compliance and exception reports.	
	Review of incidents occurred during procurement procedures.	Corrective measures taken if appropriate (cost - effectiveness criteria). Revision of procedures and/or checklists.	
	Close monitoring of physical and IT access rights to financial systems.	Yearly control on financial systems access rights.	

Relevant Control System: Revenues (Chargeback)			
Stage 1: Recognition: establishment of the Commission's rights Main internal control objectives: • Ensuring that the Commission establishes its revenue entitlements correctly and sets up its management reporting and information security • Compliance (legality & regularity) • Sound Financial Management (effectiveness, efficiency, cost-effectiveness) • Prevention of fraud (anti-fraud strategy) • Reliable Reporting (true and fair view)			
Main risks *It may happen (again)* ***that...***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
The MOUs / SLAs embed weaknesses that would undermine the Commission's legal rights in terms of revenue entitlements.	The GMoUs and SLAs are based on templates provided by the respective Commission services with expertise on the subject. Subsequently there is hierarchical validation of the agreements, with legal & financial circuits within the authorising department.	All services.	<u>Effectiveness:</u> Value of the charge-back amount. <u>Benefits:</u> The pooling of resources in order to achieve better services at a lesser cost. <u>Efficiency:</u> Know-how, capacities and resources developed can be made available for a fraction of the cost of what it would cost developing them internally or procuring them in the open market. <u>Economy (costs):</u> Cost of control of charge-back activities in this phase / Amount charged-back.
Recognition of the revenues are not done at the right moment (e.g. when they become due) or not for the right amount.	DIGIT has established a Chargeback process with a well defined workflow in terms of timing and responsibilities.	All services.	

Relevant Control System: Revenues (Chargeback)			
Stage 2: Protection: recording, follow-up and accounting of the Commission's rights Main internal control objectives: • Ensuring that the Commission establishes its revenue entitlements correctly and sets up its management reporting and information security • Compliance (legality & regularity) • Sound Financial Management (effectiveness, efficiency, cost-effectiveness) • Prevention of fraud (anti-fraud strategy) • Reliable Reporting (true and fair view).			
Main risks *It may happen* ***(again) that...***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
The implementation of the MOUs / SLAS entails weaknesses, which lead to the Commission's legal rights in terms of revenue entitlements not being duly protected and/or registered and/or reliably reported.	The Chargeback Revenue, backed by supporting documents, is recognised in the financial systems of the Commission, therefore Revenue entitlements are safeguarded by the financial systems of the Commission.	All services.	Effectiveness: Value of the charge-back amount. Benefits: The pooling of resources in order to achieve better services at a lesser cost. Efficiency: Know-how, capacities and resources developed can be made available for a fraction of the cost of what it would cost developing them internally or procuring them in the open market. Economy (costs): Cost of control of charge-back activities / Amount charged-back.

Relevant Control System: Revenues (Chargeback)			
Stage 3: Ex post – Supervisory measures Main internal control objectives: • Ensuring that any weakness in the procedures (chargeback) is detected and corrected			
Main risks *It may happen* ***(again) that...***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
An error or non-compliance with regulatory and contractual provisions, including technical specifications, or a fraud is not prevented, detected or corrected by ex ante control, prior to payment.	The chargeback process is being followed up at a detailed level that allows for specific reconciliations to be performed by multiple actors at different levels and stages of the process.	100%	Effectiveness: Value of the charge-back amount. Benefits: Amounts detected associated with error corrected. Efficiency: Estimation of cost of staff involved. Economy (costs): Cost of control of charge-back activities / Amount charged-back.

Relevant Control System: Non-expenditure items: (In)tangible Assets			
Stage 1: Recognition: establishment of the Commission's rights Main internal control objectives: • Ensuring that the Commission establishes its assets ownership and liabilities correctly and sets up its management reporting and information security • Sound Financial Management (effectiveness, efficiency, cost-effectiveness) • Prevention of fraud (anti-fraud strategy) • Safeguarding Assets (incl. accounting) • Reliable Reporting (true and fair view)			
Main risks *It may happen* ***(again) that...***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
Recognition of the assets is not done at the right moment (e.g. when they become due, when the ownership is transferred, when they become certain), or not for the right amount.	Hierarchical validation of the operation with legal & financial circuits, within the authorising department.	100%	Effectiveness: Value of the assets concerned. Benefits: The (average annual) total value of the significant errors detected/avoided - and thus prevented in terms of the Commission's rights. Efficiency: Value of assets in relation to the cost of staff involved. Economy (costs): Estimation of cost of staff involved.
	Accounting Officer verifying that AO(S)Ds establish inventory and information flow into ABAC (cf. validation of local systems).	100%	

<table>
<tr><th colspan="4">Relevant Control System: Non-expenditure items : (In)tangible Assets</th></tr>
<tr><td colspan="4">Stage 2: Protection: recording, follow-up and accounting of the Commission's rights
Main internal control objectives:
• Ensuring that the Commission registers and protects its assets ownership and liabilities correctly, reports transparently
• Compliance (legality & regularity)
• Sound Financial Management (effectiveness, efficiency, cost-effectiveness)
• Prevention of fraud (anti-fraud strategy)
• Safeguarding Assets (incl. accounting)
• Reliable Reporting (true and fair view)</td></tr>
<tr><th>Main risks
It may happen
(again) that…</th><th>Mitigating controls</th><th>Coverage frequency and depth of controls</th><th>Possible Cost-effectiveness indicators (3Es)</th></tr>
<tr><td rowspan="2">EU accounting rules are not respected regarding assets.</td><td>Clear procurement, accounting, inspection, depreciation and disinvestment rules; EU accounting rules.</td><td>For 100% of the assets.</td><td rowspan="3"><u>Effectiveness:</u>
Value of the assets concerned.
Number of findings about incorrect registration of items.
<u>Benefits:</u> Avoid the wrong imputation in accounting system and compliance with regulatory provisions.
<u>Efficiency:</u>
Value of assets in relation to the cost of staff involved.
<u>Economy (costs):</u>
Estimation of cost of staff involved.</td></tr>
<tr><td>(In)tangible assets and inventories follow formal procedure for disposal of assets.</td><td>Close follow up of inventory and depreciation.</td></tr>
<tr><td>Failing to prevent, detect and correct negligence, irregularities, errors, losses or attempted fraud.</td><td>Controls aiming at safeguarding the assets it purchases and manages on behalf of all the DGs and services of the Commission:
A. Physical check of all assets and non-assets.
B. Itemised checks when writing off obsolete, lost or damaged goods, as well as on-going registration in ABAC Assets of all logistical movements (deliveries, moves, swaps, withdrawals, etc.).</td><td>100% during the lifecycle of the items.
Physical check at least every two years.</td></tr>
</table>

Relevant Control System: Non-expenditure items: Information & IT security			
Stage 1: Protection: recording & follow-up of the Commission's rights Main internal control objectives: • Sound Financial Management (effectiveness, efficiency, cost-effectiveness) • Prevention of fraud (anti-fraud strategy) • Safeguarding Information; Reliable Reporting (true and fair view)			
Main risks *It may happen* ***(again) that…***	Mitigating controls	Coverage frequency and depth of controls	Possible Cost-effectiveness indicators (3Es)
Sensitive information is **'lost' (abused,** made public) or its integrity breached (data altered).	Internal rules on data protection in line with Commission's rule, and internal rules on treatment of sensitive information.	100%	<u>Effectiveness:</u> Nr of events during the reporting year. <u>Benefits:</u> Avoid the non-compliance with regulatory provisions and loss of information / preventing Commission's exposure. No unauthorised access. <u>Efficiency:</u> No reputational events damaging Commission. <u>Economy (costs):</u> Estimation of cost of staff involved.
	Close monitoring of physical and IT access rights to financial systems.	Yearly control on financial systems access rights.	
Sabotage, destruction of critical documents, damage to equipment, theft of high-value equipment or sensitive information by external parties / contractors.	Organisation of meetings with HR/DS to standardise and reinforce the access security measures for external staff (use of a single Information system….).	Security rules and culture to be adjusted in view of latest technical developments and 'possibilities'.	
	Security clearance for contractors when needed.	Right to clearance 100% checked.	
	Close monitoring of physical and IT access rights to financial systems.	Yearly control by ICC on financial systems access rights.	
Politically or economically motivated computer crime (hacking) to conduct sabotage or espionage against the Commission's IT systems.	Increase the Commission's capability for detection, preventive and responsive measures. Ensure that key IT security processes are implemented consistently across the Commission for main corporate IT systems. Improve global IT infrastructure security level through network and endpoint securisation and security oversight of key corporate systems.	Application of IT security governance rules Commission wide.	<u>Effectiveness:</u> Nr of events during the reporting year. <u>Benefits:</u> The number avoided breaches (annually) and thus preventing Commission's exposure. <u>Efficiency:</u> No reputational events damaging Commission. <u>Economy (costs):</u> Estimation of cost of staff involved. (DIR S of DIGIT + all various stakeholders (end-users, technical staff, decision makers).

ANNEX 7: Specific annexes related to 'financial management'

A. Free content:

In 2025, administrative expenses related to salaries and/or missions are reported by the service responsible for the commitment, although the payments were executed by another service, notably the PMO and/or DG HR ([13]), which, until 2024, also reported the corresponding expenditure. This new reporting arrangement was introduced in the context of data rationalisation linked to the implementation of the Commission's new IT accounting system. In 2025, these expenses represented 0.13% of DG DIGIT's total payments.

Digital Europe control results

Like for Horizon Europe, 2025 was the fifth year of implementation of the Digital Europe programme.

The error rates based on the results of ex post controls for the Digital Europe on 31 December 2025 are:

- **Detected error rate (DER)** for the DEP audits at family level finalised in 2025 ([14]): **2,22%**
- **Residual error rate (RER)** for the DEP audits at family level finalised in 2025: **2,21%**

As set out in the Digital Europe audit strategy ([15]), given that the number of audits will be limited during the first years of the implementation of the programme and that the resulting DEP error rate will therefore not be representative, the error rate of the Horizon Europe programme will be used as a reference for reporting purposes.

Horizon Europe has similar cost eligibility criteria and a comparable profile of beneficiaries to DEP. An analysis performed in early 2025 shows that DEP is the programme (together with Erasmus 2027) that shares the most beneficiary with HE (approx. 48% of DEP unique beneficiaries). Both programmes therefore present a relatively similar risk of error.

DG DIGIT uses 0.5% conservative estimate for administrative expenditure. Even if DG DIGIT is a Digital Europe Programme (DEP) stakeholder, the error rates calculated for DEP are not used in this AAR as 'equivalents', for the following reasons:

- The first ex post audits for Digital Europe were launched in the second half of 2024, once a meaningful number of payments was available for audit and in line with the Programme's ex post audit strategy.
- The first batch of 20 audits (corresponding to 23 participations) finalised in 2025, concerned CONNECT and HaDEA participations, no other DEP stakeholder have been audited in 2025.

([13]) Type III co-delegation.
([14]) Based on a first batch of 20 audits (corresponding to 23 participations) finalised in 2025 which concerned only CONNECT and HaDEA, no other DEP stakeholder having been audited in 2025.
([15]) Digital Europe Ex-Post Audit Strategy par. 4.5.1

- Given the fact that the number of audits is limited during the first years of the implementation of DEP and that the resulting DEP error rate will therefore not be representative, the error rate of the Horizon Europe programme should be used as a reference for reporting purposes, according to DEP ex post audit strategy.
- However, the 2024 audit campaign did not include any projects managed by DG DIGIT, as well as the 2025 DIGIT payments did not include any cost claims related to grants, except for one pre-financing. For this reason, neither the provisional error rate calculated for DEP by HaDEA is used by DG DIGIT in this AAR, nor is the error rate of Horizon Europe.

Audit coverage

Digital Europe

Like for Horizon Europe, 2025 was the fifth year of implementation of the Digital Europe programme. The first ex post audits for Digital Europe were launched in the second half of 2024 once a meaningful number of payments was available for audit and in line with the Programme's ex post audit strategy.

In its role of audit centre for the Digital Europe, HaDEA performed 20 audits (23 participations), representing just 2.25% of the total Digital Europe population at the end of 2025. As most of the audits were closed in the last quarter of 2025, efforts to implement the audit results and reduce the residual error rate are still underway and could not yet impact the reduction of the residual error rate. The goal is to focus on risk-prone areas, preventing errors and reinforce communication campaigns on eligibility rules to beneficiaries,

Actions taken to reduce the error rate on Digital Europe

The audit campaigns started and, in line with the Digital Europe Audit strategy, HaDEA performed the audit of 23 participations covering EUR 8,8 million EU contribution.

Information campaigns were organised. In particular, during the meetings with the National Contract Points of 25 June 2025 and 24 October 2025, CONNECT provided training on cost reporting with a specific focus on aspects which can be a source of errors.

Since the start of the programme, the Annotated Model Grant Agreement was regularly updated to include relevant guidance on the correct management of the grants.

CONNECT also explored the possibilities of a wider use of lump sums for Digital Europe grants given that lump sums are considered as an important tool to reduce financial errors, achieve simplification and cut administrative burden.

Fraud risk management

Objective: The risk of fraud is minimised through the application of effective anti-fraud measures and the implementation of the Commission anti-fraud strategy ([16]) aimed at the prevention, detection and correction ([17]) of fraud		
Indicator 1: Implementation of the actions included in **DG DIGIT's** anti-fraud strategy over the whole lifetime of the strategic plan (2025-2029) Source of data: DG DIGIT's anti-fraud strategy, DG DIGIT's Management Plan 2025		
Baseline (2024)	Target (2029)	Latest known results (situation on 31/12/2025)
80% of due actions implemented each year	100% of due actions implemented each year	100% of due actions implemented in 2025

Main outputs in 2025:			
Description	Indicator	Target	Latest known results (situation on 31/12/2025)
Identify and assess fraud risk and update DIGIT risk register accordingly	The risk register is updated, considering the risk of fraud	Yearly completion, by end of 2025	Target achieved Fraud risks were assessed, and the annual risk register was updated in October 2025 accordingly.
Raise fraud awareness within DIGIT (through training/information sessions)	Number of anti-fraud training/information sessions	1 session per year, by end of 2025	Target achieved A thematic ethics and integrity awareness seminar was organised in collaboration with DG HR
Strengthen fraud prevention in the procurement process	Review that the preventive actions have been followed during the year	Yearly completion, by end of 2025	Target achieved Preventive actions in the procurement area were implemented.
Strengthen ex post controls to detect potential fraud	Implement the ex post controls procedure	Yearly completion, by end of 2025	Target achieved The annual ex post controls exercise was organised and completed

([16]) Communication from the Commission 'Commission Anti-Fraud Strategy: enhanced action to protect the EU budget', COM(2019) 176 of 29 April 2019 – 'the CAFS Communication'; Communication from the Commission 'Commission Anti-Fraud Strategy Action plan – revision 2023' COM(2023) 405 of 11 July 2023 – 'the Communication on the 2023 revision' – and the accompanying revised action plan, SWD(2023) 245– 'the revised Action Plan'.

([17]) Correction of fraud is an umbrella term, which refers in particular to the recovery of amounts unduly spent and to administrative sanctions.

Description	Indicator	Target	Latest known results (situation on 31/12/2025)
Continue the implementation of action 11.A of CAFS action plan	Implementation of the actions in the European Commission Corporate Cybersecurity Strategy 2025-2026 according to the associated planning	100% of actions foreseen for 2025	Target partially achieved 80,26% of actions foreseen for 2025 was completed

B. Compulsory for all departments:

1. Reports and documentation considered for the assessment of the DG's functioning in view of the AOD's assurance:

- the reports from AOSDs;
- the contribution by the Director in charge of Risk Management and Internal Control, including the results of internal control monitoring at department level;
- the reports on recorded exceptions, non-compliance events and any cases of 'confirmation of instructions' (Art 92.3 FR);
- the reports on ex post supervision and/or audit results;
- the observations and recommendations reported by the Internal Audit Service (IAS);
- the observations and the recommendations reported by the European Court of Auditors (ECA).

2. Financial Regulation: Additional reporting requirements resulting from the 2018 and 2024 revisions.

In line with the requirements of the Financial Regulation, DG DIGIT reports for the year 2025:

- No cases of in-kind donation made to the Union, for the purposes of humanitarian aid, emergency support, civil protection or crisis management aid (FR art 25.3)
- No cases of 'confirmation of instructions' (FR art 92.3)
- No cases of financing not linked to costs (FR art 125.3)
- No cases of Financial Framework Partnerships >4 years (FR art 131.4)
- No cases of flat-rates >7% for funding indirect costs (FR art 184.6)
- No cases of derogations from the principle of non-retroactivity pursuant to Article 196 of the Financial Regulation.
- No cases of financial support to third parties >EUR 60 000 (FR art 207)
- No cases of non-financial donations provided in the form of services, supplies or works (FR art 244.3)

3. Table Y on the estimated 'cost of controls' at Commission level

Overview of DG DIGIT's estimated cost of controls at Commission (EC) level

EXPENDITURE

The absolute values are presented in EUR

DIGIT	Ex ante controls***			Ex post controls			Total	
	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
Segment of expenditure (as in Table X) / Relevant Control System (RCS) / Other as defined in Annex 6 of the AAR*	EC total costs	related payments Made	Ratio (%)** *(a)/(b)*	EC total costs	total value verified and/or audited	Ratio (%) *(d)/(e)*	EC total estimated cost of controls *(a)+(d)*	Ratio (%)** *(g)/(b)*
Procurement	2.435.360,00 €	3.527.236.575,68 €	0,07%	- €	- €	0,00%	2.435.360,00 €	0,07%
Commitments	2.452.630,00 €	626.859.795,89 €	0,39%	- €	- €	0,00%	2.452.630,00 €	0,39%
Payments	962.620,00 €	618.294.110,34 €	0,16%	17.815,00 €	22.386.499,50 €	0,08%	980.435,00 €	0,16%
OVERALL total estimated cost of control at EC level for expenditure	**5.850.610,00 €**	4.772.390.4**81,91 €**	0,12%	**17.815,00 €**	**22.386.499,50 €**	0,08%	**5.868.425,00 €**	0,12%

NON-EXPENDITURE ITEMS ****

DIGIT	Ex ante controls***			Ex post controls			Total	
	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
Segment of expenditure (as in Table X) / Relevant Control System (RCS) / Other as defined in Annex 6 of the AAR*	EC total costs	related amounts	Ratio (%)** *(a)/(b)*	EC total costs	total value verified and/or audited	Ratio (%) *(d)/(e)*	EC total estimated cost of controls *(a)+(d)*	Ratio (%)** *(g)/(b)*
Only applicable for DGs with non-expenditure items								
Chargeback	328.930,00 €	341.656.624,39 €	0,10%	21.790,00 €	341.656.624,39 €	0,01%	350.720,00 €	0,10%
Assets (including Access rights)	288.874,00 €	17.816.841,10 €	1,62%	118.966,00 €	17.816.841,10 €	0,67%	407.840,00 €	2,29%

** if the control costs are not attributable to a single RCS and may relate to a 'mix' of expenditure, revenue, assets/liabilities, etc, they may be grouped*
*** ratio possibly "Not Applicable (N/A)", e.g. if a RCS specifically covers an Internal Control Objective such as safeguarding sensitive information, reliable accounting/reporting, etc*
**** any 'holistic' control elements (e.g. with 'combined' ex-ante & ex-post characteristics) can be reported in the ex-ante column provided that a footnote clarifies this (their nature + their cost). Example: MS system audits in shared management.*
***** These include revenue operations (e.g. assigned revenue, fines, interest); assets (e.g. (in)tangible or financial assets, inventories, treasury) and financial liabilities or 'off balance sheet' items (e.g. employee benefits, guarantees offered or other commitments)*

While Table X includes only the amount of the payments made, Table Y contains all relevant segments of expenditure which are controlled ex ante and, if applicable, ex post, i.e. procurement, commitments, and payments. This explains the difference in the payments declared between Table X and Table Y.

Details of the estimated cost of the control activities related to payments for salaries and/or missions executed by DG HR/PMO are reported in their respective annual activity reports.

4. Financial corrections and recoveries, suspensions and interruptions of payments carried out during the reporting year per Member State, programming period and fund

Not applicable for DG DIGIT.

5. Preventive and corrective measures as a result of ex ante and ex post controls.

		Preventive Measures (m EUR)	Corrective measures (m EUR)
Implemented by the Member States:			
	of which from Member States controls	*NA*	*NA*
	of which from EU controls **([18])**	*NA*	*NA*
Implemented by the Commission			
	of which from Member States controls	*NA*	*NA*
	of which from EU controls	*0*	*0*
DG DIGIT total			

([18]) As a result of Commission controls and audits (including additional corrections to ensure a risk at closure below 2% in case of EMPL, REGIO and MARE), OLAF investigations or ECA audits.

ANNEX 8: Reporting on the internal and external audits and assessing the effectiveness of internal control systems

Internal audit service (IAS)

Audits finalised in DG DIGIT in the period 2021-2025 ([19])

- Audit on IT security management in the HR family (DIGIT, HR, PMO, EPSO) (2021);
- Audit on the management and monitoring of compliance with the Commission's IT security framework (2021);
- Audit on progress in the implementation of the European Commission digital strategy (2022);
- Audit on physical security of persons and assets in the Commission (HR, COMM, OIB, OIL, DIGIT) (2022);
- Audit on public procurement in DG DIGIT (2022);
- Audit on the protection of confidentiality of information at corporate level (HR, SG, DIGIT) (2023);
- Audit on the IT financing framework in DG DIGIT (2024);
- Audit on IT security risk management at the Commission (DIGIT, AGRI, CNECT, DGT, ECHO, ENER, MARE, OLAF, OP, RTD, SANTE, TRADE) (2024);
- Arachne+ project in DG BUDG, DG DIGIT, DG EMPL, DG REGIO (2025).

Open recommendations issued rated as 'very important'

Audit on IT financing framework in DG DIGIT (2024)

The objective of this audit was to assess the adequacy of the design and the effective implementation of the control framework put in place by DG DIGIT for the management of the baseline IT services and of the charge-back processes, including the adequacy of the tools to effectively monitor and report on these activities, and whether the current IT financing framework is adequate to enable DG DIGIT to deliver sustainable corporate IT services going forward.

The final audit report was received at the end of October 2024.

([19]) Final audit reports issued in the period 1 February 2021 – 31 January 2025.

The IAS noted the significant progress made by DG DIGIT in the last few years to drive and facilitate the digital transformation of the Directorates-General (DGs) and of the Commission as a whole, exploiting the capabilities offered by the digital technologies.

The IAS issued one recommendation rated as 'very important' addressed to DIGIT.

DG DIGIT prepared and submitted an action plan, which was accepted by the IAS, in January 2025. DIGIT is currently implementing the action plan.

The initial target date (Q2 2025 for the 'very important' recommendation) has been revised to end 2026, to allow for a more in-depth review of the revised IT financing framework and to test its implementation. The impact of this postponement is considered very limited, since the new MFF is not yet adopted, and the actions which are being putting in place to address the other recommendations stemming from this audit ensure continuity and enhancement of the current IT financing framework.

IAS 'very important' recommendation	Measures implemented by DIGIT
Rec. 1 – The concept of baseline IT services and the adequacy of the current IT financing framework	DG DIGIT has worked on a model concept paper for a revised IT financing framework, in coordination with SG and DG BUDG. Work is ongoing to include detailed figures in the proposal, to understand its impacts and so that DGs can properly assess and anticipate future funding model.

Audit on IT security risk management at the Commission (DIGIT, AGRI, CNECT, DGT, ECHO, ENER, MARE, OLAF, OP, RTD, DG SANTE, TRADE) (2024)

The objective of the audit was to provide assurance on the adequacy of the design, the efficiency and the effectiveness of the IT security risk management (ITSRM) framework (methodologies, standards, guidelines and tools) and processes at the corporate (Commission) and at the decentralised (department) level, thus ensuring compliance with the EC IT security framework and international best practices.

The final audit reports ([20]) were received at the end of January 2025.

The IAS concluded that, although the Commission has designed an adequate ITSRM framework and processes, in compliance with the Commission IT security framework, very important weaknesses regarding the ITSRM methodology and related tools, the risk acceptance criteria, the monitoring and reporting of the risk assessment results, and the completeness and accuracy of IT security information, affect their effective and efficient implementation.

The IAS issued six recommendations rated as 'very important' addressed to the Commission for which DIGIT is in charge, and one recommendation rated as 'very important' addressed directly to DIGIT. These recommendations do not have a material impact on the effectiveness of the

([20]) Two final reports were addressed to DIGIT, one at 'Commission' level, and one at 'department' level.

internal control system and achievement of the internal control objectives. Hence, they do not lead to reservations.

DG DIGIT prepared and submitted the action plans, which were accepted by the IAS, in April 2025. DIGIT is currently implementing the action plans, which are due to be completed by end 2026.

IAS 'very important' recommendation	Measures implemented by DG DIGIT
Rec. 1 – IT security risk management methodologies	The Commission's ITSRM framework will be complemented by a list of acceptable ITSRM methodologies and their related tools, and guidance will be provided so that risk assessment results can be measured against a common risk scale.
Rec. 2 – Quality of ITSRM	A quality assessment guidance for risk studies and IT security plans will be developed.
Rec. 3 – Guidance and supporting tools	The development plan for the technical implementation of the requested features in the supporting tool was produced. The guidance on how to address the specific tool limitations identified in the finding was issued.
Rec. 6 – Risk appetite and acceptance criteria	Guidelines on the 'Integrated corporate, business and IT risk management' were drafted. In view of conducting a thorough consultation on the drafted guidelines, the initial target date of this recommendation was revised to Q1 2026.
Rec. 7 – IT security monitoring and reporting	A note addressed to the DGs and Executive Agencies was issued, on the role of the Local Informatics Security Officer (LISO) and the responsibilities of System Owners.
Rec. 8 – Completeness and accuracy of IT security information	A revised guidance for the IT security indicators containing suggested Internal Control Monitoring Criteria (ICMC) related to internal control principle 11 was developed. A note was issued, detailing the mandatory consultation of important stakeholders at each step in the IT security risk management process.
Rec. 1 – IT security risk management methodologies and tools	IT security risk studies and IT security plans for the audited tools will be updated.

Arachne+ project in DG BUDG, DG DIGIT, DG EMPL, DG REGIO (2025)

The objective of the audit was to assess whether DG BUDG, DG EMPL/DG REGIO (DAC) and DG DIGIT had put in place appropriate governance, risk management and control processes to deliver the Arachne+ project - phase 2 effectively, achieve the strategic objectives and business expectations within the allocated time and resources, and be in compliance with the Commission's security and personal data protection framework.

The final audit report was received at the end of November 2025.

The IAS concluded that, although governance, risk management and control processes had been established for Arachne+, they were not sufficiently appropriate to deliver the phase 2 of the project effectively. IT security and personal data protection control processes were compliant with the Commission's process steps, though improvements are necessary as regards the quality of IT security artefacts.

The IAS issued two recommendations rated as 'very important' addressed to DIGIT.

The audited DGs prepared and submitted an action plan, which was accepted by the IAS, in February 2026, and are currently implementing it according to the agreed target dates (Q2 and Q4 2026 for the 'very important' recommendations addressed to DG DIGIT), therefore mitigating the risks identified.

IAS 'very important' recommendation	Measures to be implemented by DIGIT
Rec. 3 – Support project owner from the **solution provider's perspective**	DG DIGIT will support DG BUDG by participating in the meetings of the Business Working Group and its sub-groups. DG DIGIT, together with BUDG, will discuss and implement enhanced reporting on the progress of the Arachne+ project towards delivery.
Rec. 7 – Implement the defined IT security measures and ensure risk acceptance criteria have been satisfied	Implement the security measures before Arachne+ Service Activation. Conduct the risk study as part of the new version of the IT security plan, following the new business impact assessment.

European Court of Auditors (ECA)

Statement of Assurance

The ECA is performing its yearly statement of assurance (DAS) exercise related to the reliability of the accounts and the legality and regularity of the underlying transactions. Within the DAS 2025 exercise, a sample of 16 transactions involving DG DIGIT – either as the service responsible for the sampled transaction, or because the sampled transaction was executed under a framework contract managed by DG DIGIT – is being examined. For the moment, no specific issues have been communicated to DG DIGIT.

For DAS 2024, DG DIGIT is implementing recommendation 10.1 stemming from the 2024 Annual Reports on the implementation of the EU budget for the 2024 financial year and on the activities funded by the 9th, 10th and 11th European Development Funds (EDFs) for the 2024 financial year.

Performance audits

In 2025, the ECA conducted the follow-up of the recommendations stemming from SR 05/2022 and SR 18/2022. No audits involving DG DIGIT were conducted by the ECA in 2025.

ANNEX 9: Specific annexes related to ‘Control results’ and ‘Assurance: Reservations’

A. Annex related to ‘Control results’ - Table X: Estimated risk at payment and at closure

Table X: Estimated risk at payment and at closure

DG DIGIT *-1*	Payments made (2025;MEUR) *-2*	minus new prefinancing [plus retentions made] (in 2025;MEUR) *-3*	plus cleared prefinancing [minus retentions released and deductions of expenditure made by MS] (in 2025;MEUR) *-4*	Relevant expenditure (for 2025;MEUR) *-5*	Detected error rate or equivalent estimates *-6*	Estimated risk at payment (2025;MEUR) *-7*	Adjusted Average Recoveries and Corrections (*adjusted* ARC; %) *-8*	Estimated future corrections [and deductions] (for 2025;MEUR) *-9*	Estimated risk at Closure (2025;MEUR) *-10*
RCS 1 - Procurement and administrative expenditure	619,10	- 2,40	0,00	616,70	0,00% - 0,50%	0,00 - 3,08	0,00% - 0,00%	0,00 - 0,00	0,00 - 3,08
DG total	619,10	- 2,40	0,00	616,70		0,00 - 3,08	0,00% - 0,00%	0,00 - 0,00	0,00 - 3,08
					Overall risk at payment in %	0,00% - 0,50% *(7) / (5)*		Overall risk at closure in %	0,00% - 0,50% *(10) / (5)*

Notes to the table X

(1) Different segments of Relevant Control System 1 described in Annex 6 are broader than payments made. For the purpose of calculation of estimated risk at payment and at closure, DG DIGIT considers more pertinent to focus on the amount of payments made.

(2) Payments made after the preventive (ex-ante) control measures have already been implemented earlier in the cycle. For Cross-SubDelegations (Internal Rules Article 12), the reporting remains with the Delegating departments.
RCS 1 covers/includes administrative expenses related to salaries and/or missions previously reported by the PMO and/or DG HR. More information can be found in Annexes 6 and 7.

(3) New pre-financing actually paid by out by the department itself during the financial year (i.e. excluding any pre-financing received as a transfer from another department). as per note 2.5.1 to the Commission annual accounts thus excluding ‘Other advances to Member States’ which are covered on a purely payment-made basis (note 2.5.2). Pre-financing paid/cleared’ are always covered by the Delegated departments, even for Cross-SubDelegations.
Retentions: in Cohesion, the 10% retention applied during the year.

(4) Pre-financing actually cleared during the financial year (i.e. their 'delta' in the Financial Year 'actuals', not their 'cut-off' based estimated 'consumption'). Retentions: in Cohesion, the retentions released during the year by the Commission.

(5) For the purpose of equivalence with the ECA's scope of the EC funds with potential exposure to legality & regularity errors (see the ECA's Annual Report methodological annex 1.1), our concept of ‘relevant expenditure’ includes the payments made, subtracts the new pre-financing paid out [& adds the retentions made], and adds the pre-financing

actually cleared [& subtracts the retentions released; and any deductions of *expenditure made by MS*] during the FY. This is a separate and 'hybrid' concept, intentionally combining elements from the budgetary accounting and from the general ledger accounting.

(6) In this column, we disclose the detected error rates or equivalent estimates. For low-risk types of expenditure, where there are indications that the equivalent error rate might be close to 'zero' (e.g. administrative expenditure, operating contributions to agencies), the rate which should be used is 0.5% as a conservative estimate, unless the department has a more precise estimate based on evidence.

DG DIGIT uses 0.5% conservative estimate for administrative expenditure. Even if DG DIGIT is a Digital Europe Programme (DEP) stakeholder, the error rates calculated for DEP are not used in this AAR as 'equivalents', for the following reasons:

- The first ex post audits for Digital Europe were launched in the second half of 2024, once a meaningful number of payments was available for audit and in line with the Programme's ex post audit strategy.
- The first batch of 20 audits (corresponding to 23 participations) finalised in 2025, concerned CONNECT and HaDEA participations, no other DEP stakeholder have been audited in 2025.
- Given the fact that the number of audits is limited during the first years of the implementation of DEP and that the resulting DEP error rate will therefore not be representative, the error rate of the Horizon Europe programme should be used as a reference for reporting purposes, according to DEP ex post audit strategy.
- However, the 2024 audit campaign did not include any projects managed by DG DIGIT, as well as the 2025 DIGIT payments did not include any cost claims related to grants, except for one pre-financing. For this reason, neither the provisional error rate calculated for DEP by HaDEA is used by DG DIGIT in this AAR, nor is the error rate of Horizon Europe.

(8) The adjusted average recovery and corrections percentage is based on the 7 years historic Average of Recoveries and financial Corrections (ARC), which is the best available indication of the corrective measures each department applied over the past years as a result of ex post controls. The AOD has adjusted this historic average 0.5% to 0% to take into account any ex ante elements, one-off events, (partially) cancelled or waived Recovery Orders, and other factors from the past years that would no longer be relevant for the current programmes (e.g. higher ex post corrections of previously higher errors in earlier generations of grant programmes, current programmes with entirely ex ante control systems) or that corresponded to exceptional situations in order to come to the best and most conservative estimate of the ex post future corrections to be applied to the reporting year's relevant expenditure for the current programmes.

DG DIGIT can estimate that future corrections will be higher than 0 MEUR, given that ex post audits for the programmes of the current MFF, notably DEP, will be finalised and their results will be implemented in the years to come (the audit campaigns were started during 2024), leading to future corrections. In the first years of the DEP, there was not a meaningful number of payments available for audit, and consequently there were no implemented corrections for DG DIGIT. On a regular basis, HaDEA will perform ex post audits, as well as perform an analysis of the audit findings deriving from the execution of the DEP ex post audit strategy and share it with the DEP stakeholders. The aim is to identify and correct errors earlier in the project lifecycle, draw attention to relatively riskier areas, in view to aim to prevent errors, improve the ex ante controls and ultimately reduce the residual error rates of the programme.

(9) For some programmes with no set closure point (e.g. EAGF) and for some multiannual programmes for which corrections are still possible afterwards (e.g. EAFRD and ESIF), all corrections that remain possible are considered for this estimate. N/A for DG DIGIT.

B. Reservations

1. Reservation fiche

Not applicable.

2. Reservations not issued or lifted in 2025 due to the application of the ‘de minimis’ threshold.

Not applicable.

ANNEX 10: Reporting – Human resources, digital transformation and data management, and sound environmental management

Human Resource management

Objective: DIGIT employs a skilled, diverse and motivated workforce to deliver on the Commission's priorities		
Indicator 1: Percentage of female middle managers Source of data: SYSPER		
Baseline (2024)	Target (2029)	Latest known results (situation on 31/12/2025)
42%	50%	44% (8/18)
Indicator 2: Staff engagement index Source of data: Commission staff survey 2025, data provided by DG HR		
Baseline (2023)	Target ([21]) (2029)	Latest known results ([22]) (situation on 31/12/2025)
75%	maintain or increase	New Staff Engagement Index (2025): 83% Old Staff Engagement Index (2023): +1 percentage points

Main outputs in 2025:			
Description	Indicator	Target	Latest known results (situation on 31/12/2025)
Targeted follow-up actions in areas for improvement identified in the latest staff survey	Number of follow-up actions / events	Organise at least 3 follow-up actions / events, by end of 2025	Target achieved. Nineteen actions took place; with these three being the most significant: - Well-being week 23-26/9/25; - Two sessions organized with the Confidential Counsellor (one for staff and one for management); - Two sessions on career development (one on 'Learning Packages' and one on 'Shaping your Career').

([21]) The Commission baseline score for the Staff Engagement Index is 73% (based on the 2023 staff survey results).

([22]) A new method of measuring staff engagement was introduced in 2025. The new Staff Engagement Index provides a more comprehensive view of staff engagement covering purpose, pride and motivation, autonomy and growth and collaboration and trust. The old Staff Engagement Index, which focused more on job content and relations with immediate colleagues and manager, will be used exclusively for comparisons with past data.

Description	Indicator	Target	Latest known results (situation on 31/12/2025)
Leadership development: Provide leadership training / coaching to aspiring managers, specifically encouraging female staff to participate	Number of leadership trainings / coachings offered	Offer at least 2 leadership trainings to DIGIT staff, by end of 2025	Target achieved. Five actions were implemented by DIGIT in the domain of leadership development ([23]): - One DHoU (male) and one HoS (female) joined the Management Development Programme for future Middle Managers in 2025; - One staff member (female) attended the training by the Oxford Management Centre on Artificial Intelligence (AI) for Leaders and Managers; - One staff member (male) attended the training on Disruptive Strategy by the Harvard Business School; - Two staff members (female) attended the training on Strategy in the Age of AI and Digital Disruption by the Harvard Business School; - The Interinstitutional Women in IT Network started in 2025, led by DIGIT, and chaired by the Director (female) of Change Management and Resources at DG DIGIT.

Digital transformation and data management

Objective: DIGIT is using innovative, trusted digital solutions for better policymaking, data management and administrative processes to build a digitally transformed, user-focused and data-driven Commission			
Indicator 1: Digital Culture: % of statutory staff that has completed at least one IT training course ([24]) Source of data: Digital Commission Dashboard (data measured at DG-level)			
Baseline (2024)	Interim milestone (2027)	Target (2029)	Latest known results (situation on 31/12/2025)
44%	45% [1 percentage point increase compared to baseline]	50% [6 percentage points increase compared to baseline]	37%

([23]) Additional leadership trainings are offered at corporate level. For instance, the European School of Administration offers a wide variety of trainings for aspiring managers, management and senior management.

([24]) This indicator measures annual participation in the Digital Skills Training Centre on the Commission's internal learning platform. A low result might indicate that staff already completed relevant trainings and have no more need (i.e. a desirable outcome).

Indicator 2: Seamless digital environment: cloud adoption – % of IT systems utilising cloud infrastructure services compared to the total number of IT systems Source of data: Digital Commission Dashboard (- data measured at DG-level)			
Baseline (2024)	Interim milestone (2027)	Target (2029)	Latest known results (situation on 31/12/2025)
20%	35% [75% increase compared to baseline]	45% [125% increase compared to baseline]	30% [50% increase compared to baseline]
Indicator 3: Maturity level in implementing corporate data policies across four key areas: data management, ownership and responsibilities, data quality, and data skills (basic, developing, established, advanced, or trendsetting). Source of data: DIGIT			
Baseline (2024)	Interim milestone (2027)	Target (2029)	Latest known results (situation on 31/12/2025)
Developing	Established	Advanced	Developing
Indicator 4: Compliance indicator ([25]): percentage of staff trained on data protection compliance combined with the percentage of public records of processing operations reviewed within the last two years. Source of data: DIGIT			
Baseline (2024)	Interim milestone (2027)	Target (2029)	Latest known results (situation on 31/12/2025)
70%	>90%	100%	80%
Main outputs in 2025:			
Digital transformation			
Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Enhance IT Portfolio Management processes and tools: development	Minimum Viable Product (MVP) is delivered	By end of 2025	Target achieved.

([25]) The compliance indicator is calculated with a 50% weight attributed to the following two values: first, the number of public records with a publication date within the last 2 years / public records of the department. Second, the percentage of staff in the department who have attended data protection awareness-raising activities

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Service Management	Service Catalogue v2 is in production	By end of 2025	Delayed. The technical implementation of the service catalogue is finalised, the go-live is postponed to Q2 2026, due to several outstanding dependencies.
Change management initiatives in DIGIT	Complete pilot of shared drives phase-out in selected processes	By end Q3 2025	Target achieved.
Data management			
Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Ownership and responsibilities dimension: Improve awareness and accountability in data management, by reporting quarterly to DIGIT Senior Management on data management maturity in DIGIT (incl. updates to key data assets, data ownership and data reusability)	Report is delivered to DIGIT Senior Management, at least 4 reports per year, starting from June 2025	By end of 2025	Target achieved. Reports are provided quarterly, including portfolio management and data management aspects.
Data protection			
Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Provide training for newcomers on data protection awareness	12 training sessions	By end of 2025	100% of the training sessions were completed, attended by 60% of newcomers

Output	Indicator	Target	Latest known results (situation on 31/12/2025)
Provide ad hoc advisory on data protection principles and compliance to staff, by means of dedicated session on data protection records (DPMS), privacy statements, data subject rights request and personal data breaches	% of requests for advisory are dealt with	95%	100%
Percentage of public records of processing operations reviewed within the last two years	% of records reviewed within 2 years	50%	65%

Sound environmental management

Objective: Reaching climate neutrality by 2030 and a reduced environmental footprint for the Commission.		
Indicator: % reduction in emissions from staff professional travel (t CO_2eq). Source of data: PMO DWH Qlik Sense dashboard ([26])		
Baseline (2019)	Target (2030)	Latest known results (situation on 31/12/2025)
193.81 t CO_2eq	50% of reduction	92.05 t CO_2eq, i.e. reduction of 52.51% (excluding College-related missions and CERT-EU missions deriving from the implementation of its annual work programme). In 2025, DIGIT took over the provision of IT services at the Commission's Representations, which created the need for additional staff travel and therefore added a new source of emissions that did not exist in 2019. These emissions have been included in the figure above. Moreover, in 2025 DIGIT was requested to start providing in-person IT support to the President and the College during their missions. These additional emissions have not been included in the overall figure above. If they were taken into account, the overall reduction would be 35.95%.

([26]) In the Management Plan 2025 the data source was specified as MIPS+. As of the current report, these emissions are reported not through MIPS+ anymore, but thought Qlik Sense. The baseline value for DIGIT is unaffected by this change in reporting.

Main outputs in 2025:			
Description	Indicator	Target	Latest known results (situation on 31/12/2025)
Actions to reduce emissions from staff missions: - Internal communication campaigns promoting more sustainable travel options - Reduce staff professional travel emissions (2030 objective)	 Deliver at least one internal communication campaign promoting more sustainable travel options Reduce CO2 emissions from missions by 50% compared to 2019 baseline	 By end of 2025 By end of 2025	Target achieved. - In 2025, the Commission published the New Mission Guide, including guidelines on greening staff travel. DIGIT promoted the guide via its internal communication channels - Reduction of 52.51% (excluding College-related missions)
Energy saving actions	Number of the annual BEST energy saving actions (coordinated by OIB) in which DIGIT premises in L107 participate	Three actions in 2025: - End of year energy saving action; - Summer energy saving action; - Optimisation of comfort hours and comfort temperature.	Target achieved. DIGIT's premises were part of the three energy saving actions centrally promoted by OIB. During the summer and end of year actions DIGIT's buildings served as hubs for colleagues from other DGs.
Staff awareness actions	Deliver at least one staff awareness action in line with EMAS/greening corporate campaigns	By end of 2025	Target achieved. In 2025, DIGIT (co-)created and promoted seven EMAS/greening awareness-raising actions on topics such as: ICT waste reduction, AI energy use, sustainable transportation and digital environmental footprint.

Description	Indicator	Target	Latest known results (situation on 31/12/2025)
Sustainable events	DIGIT events incorporating the EC guidelines for sustainable events, as percentage of all DIGIT events	100% of 2025 events	Target achieved. 100% of DIGIT's events incorporated the EC guidelines for sustainable events. Hybrid events are highly encouraged in order to reduce travel-related emissions.

ANNEX 11: Implementation through non-EU entrusted entities ([27]) and/or through EU Trust Funds

Not applicable

ANNEX 12: EAMR of the Union Delegations

Not applicable

ANNEX 13: Decentralised agencies and other Union bodies

Not applicable

ANNEX 14: Reporting on the Recovery and Resilience Facility

Not applicable

([27]) Implementing partners other than EU institutions or Union bodies.