



2019

Annual Activity Report

DG DIGIT



Table of Contents

| | |
|---|-----------|
| THE DG IN BRIEF | 3 |
| EXECUTIVE SUMMARY | 5 |
| A) KEY RESULTS AND PROGRESS TOWARDS THE ACHIEVEMENT OF THE COMMISSION'S GENERAL OBJECTIVES AND DG'S SPECIFIC OBJECTIVES (EXECUTIVE SUMMARY OF SECTION 1)..... | 5 |
| B) KEY PERFORMANCE INDICATORS (KPIs) | 10 |
| C) KEY CONCLUSIONS ON FINANCIAL MANAGEMENT AND INTERNAL CONTROL (EXECUTIVE SUMMARY OF SECTION 2.1) | 11 |
| D) PROVISION OF INFORMATION TO THE COMMISSIONER(S)..... | 11 |
| 1. KEY RESULTS AND PROGRESS TOWARDS THE ACHIEVEMENT OF THE COMMISSION'S GENERAL OBJECTIVES AND DG'S SPECIFIC OBJECTIVES | 12 |
| 2. ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL | 22 |
| 2.1 FINANCIAL MANAGEMENT AND INTERNAL CONTROL | 22 |
| 2.1.1 CONTROL RESULTS..... | 23 |
| 2.1.2 AUDIT OBSERVATIONS AND RECOMMENDATIONS | 37 |
| 2.1.3 ASSESSMENT OF THE EFFECTIVENESS OF INTERNAL CONTROL SYSTEMS | 42 |
| 2.1.4 CONCLUSIONS ON THE ASSURANCE | 44 |
| 2.1.5 DECLARATION OF ASSURANCE..... | 47 |
| DECLARATION OF ASSURANCE | 48 |
| 2.2 OTHER ORGANISATIONAL MANAGEMENT DIMENSIONS | 49 |
| 2.2.1 HUMAN RESOURCE MANAGEMENT | 49 |
| 2.2.2 INFORMATION MANAGEMENT ASPECTS..... | 49 |
| 2.2.3 EXTERNAL COMMUNICATION ACTIVITIES..... | 50 |

THE DG IN BRIEF

To enable the Commission to deliver EU policy better, more efficiently and more productively, fully seizing the opportunities offered by new technologies is the core mission of the Directorate General for Informatics (DIGIT). As leader in the ICT domain, DIGIT provides digital services supporting the European Institutions (and the Commission in particular) in their daily work.

Based in Luxembourg and Brussels, it employs 511 full time staff and manages a budget of 232 million EUR covering the provision of IT, telecommunication equipment and solutions, information systems and infrastructure services. Additionally, DIGIT has been running the IT procurement operation, which implied a growing responsibility for the Commission as IT procurement clearing house for the EU Institutions.

The DG is organised into five Directorates and the Computer Emergency Response Team (CERT-EU¹). For practical reasons, each Directorate focuses on a specific cluster of services (Business Architecture, IT equipment and support, hybrid cloud, interoperability solutions, data centres, cybersecurity, etc.), but in fact DIGIT staff is fully committed to the achievement of its priorities through an increasingly cross-cutting collaboration.

In a fast-changing political, economic and social environment, DIGIT's contribution has been pivotal for the policy-making process of the European Institutions. The work DIGIT performed in terms of digital delivery since the launch of its 2016-2020 Strategic Plan had a significant impact not only across the Commission, but also among a **wider range of stakeholders**, including other EU bodies, Member States, public authorities and public administrations. The **ISA² programme²**, managed by DIGIT, has developed interoperable solutions for more cost-effective European public administrations, as well as interoperable cross-border services for citizens and businesses.

DIGIT has been providing high quality and effective solutions that have started to transform the EU Institutions **workplace**, their **way of conducting business**, and their **supporting infrastructure**. For the past four years already, the **Commission's staff has benefited from new ways of working and collaborating**, while **secure business solutions and reliable, cost-effective infrastructures** reflect a strong alignment between IT investments and business priorities and value for money.

In the past, DIGIT has calibrated its programs and actions based on the principles inspired by the **Ministerial Tallinn Declaration on eGovernment³**, and contributed – through the implementation of interoperability principles – to the **'Connected Digital Single Market⁴'**, one of the pillars of the **'Digital Agenda for Europe'** framed in the **Europe 2020 Strategy**, and one of the 10 priorities of the Juncker Commission.

As a response to emerging technological and digital challenges, and as a further step in the pursuit of its mandate as leader of the digital transformation, DIGIT has spearheaded the development and agreement of a **digital strategy** for the Commission (**ECDS⁵**). The ECDS sets out additional goals and milestones for continuing the development of the Commission towards its future as digitally transformed, user-centric and secure data-driven public administration – the **digital Commission**.

Since the ECDS's endorsement by the College in November 2018, the principles and priorities defined in the ECDS have been running in parallel with the five strategic priorities set in the Strategic Plan 2016-2020, and DIGIT's internal work has been planned based on existing milestones and targets for both strategies. The introduction of

¹ CERT-EU (Computer Emergency Response Team) is an inter-institutional body first established in 2012. It is administratively attached to DIGIT, but draws up its work plan separately, and reports to an inter-institutional steering board.

² ISA²: Interoperability solutions for public administrations, businesses and citizens - https://ec.europa.eu/isa2/eif_en

³ <https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration>

⁴ [Digital Single Market](#)

⁵ [European Commission Digital Strategy](#)

the ECDS has determined a fundamental change to the shape of the digital delivery: while DIGIT remains the main driver of the digital transformation across the Commission, a new delivery model facilitates co-creation among all stakeholders. This means that the steps to put in place in order to achieve the transformation of the Commission will be shared among all services.

Other relevant developments :

Change of AOD

Following the decision of 04/03/2020 the College appointed Mr Mario Campolargo as Acting Director General of DIGIT starting on 16/03/2020. In accordance with the procedures for the change of Director General foreseen in the guidelines of 12/05/2016 a hand-over note on the state of play in the areas of Strategic Planning & Programming and Internal Control was sent on 12/03/2020.

In the event of a change of authorising officer by delegation (succession or transfer of some activities from one authorising officer by delegation to another), the outgoing authorising officer by delegation shall draw up for the successor or replacement a declaration setting out the state of ongoing cases.

The outgoing Director General, Mrs Gertrud Ingestad, left a handover note signed on 12/03/2020. A dialogue between Mrs Ingestad and Mr Campolargo took place on 11th March 2020 and no formal observations were made.

Furthermore it concluded that the outgoing Director General Mrs Gertrud Ingestad had reasonable assurance that the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions. This reasonable assurance was based on her own judgement and on the information at her disposal which is contained in the handover note and in its annexes. She confirms furthermore that she is not aware of anything not reported in that note which could harm the interests of the institution.

EXECUTIVE SUMMARY

This Annual Activity Report is a management report of the Director-General of DG DIGIT to the College of Commissioners. Annual Activity Reports are the main instrument of management accountability within the Commission and constitute the basis on which the College takes political responsibility for the decisions it takes as well as for the coordinating, executive and management functions it exercises, as laid down in the Treaties⁶.

a) Key results and progress towards the achievement of the Commission's general objectives and DG's specific objectives (executive summary of section 1)

The core activities of the DG focused on the achievement of the targets identified in the 2019 Management Plan, and grouped around the **11 specific objectives** framed in the Strategic Plan 2016-2020. During 2019, DIGIT also implemented concrete actions related to the **European Commission Digital Strategy**. Most of DIGIT efforts in this domain were canalised to support the other Directorates-General in defining their plans for the modernisation of **Digital Solutions** supporting their business needs. In the first quarter of 2019, DIGIT delivered the preliminary version of a 'starter kit' designed to provide guidance to other Directorate Generals during the process of elaborating their individual initiatives. Following the decision of the Information Technology and Cybersecurity Board, DIGIT has also been providing assistance to a first wave of Directorate Generals (DG BUDG, DG HR and SG), by establishing a series of workshops at senior management level. DIGIT completed the strategic analysis of the European Commission's core administration, also updating the portfolio of building blocks with the inclusion of innovative enablers. However, the corporate **Digital Solutions Modernisation Plan** was not fully achieved by end of 2019, and will be finalised in 2020, when fundamental contributions from Directorate Generals belonging to policy families will become available. One of the biggest challenges of the digital transformation and modernisation process within the Commission is the distributed nature of digital investments and decisions, meaning that Commission-wide change requires large-scale collaboration and coordination. The political changes deriving from the appointment of the new Commission also played a role in delaying this process. In addition many DGs must wait for the finalisation of the Multiannual Financial Framework 2021-2027, before being able to provide an estimate of their needs and capabilities in terms of IT modernisation. Today, policy DGs are mainly concentrating on aligning their existing IT solutions to the requirements of the next MFF with a view of ensuring continuity. Decisions on future strategic IT investments will be made in function of the MFF's policy programmes and actions and the assigned budgets.

During the first semester, DIGIT also dedicated considerable efforts to updating and renewing existing strategic frameworks. This was the case for the **Synergies and Efficiencies Initiative**, revamped through the **Communication on Stock Taking and Way forward**⁷, adopted by the Commission in March 2019. The overhauling process of the Synergies and Efficiencies Initiative coincided with a retrospective analysis of achievements and challenges related to the ICT domain of the Commission. This triggered a systematic review of persisting ICT-related constraints that require an adequate response in order to release the full potential of the technology transformation led by DIGIT.

Featured in the digital infrastructure strand of the ECDS, and pivotal for the

⁶ Article 17(1) of the Treaty on European Union.

⁷ <https://ec.europa.eu/transparency/regdoc/rep/3/2019/EN/C-2019-2329-3-EN-MAIN-PART-1.PDF>

Commission's digital transformation, the Commission's **Cloud Strategy**⁸ (approved by the ITCB in May 2019) has introduced new paradigms into the IT landscape. At the core of the Strategy is a '**cloud-first**' approach, which is in turn tightly linked with the '**cloud native**' principle. This implies that new applications and other technological innovations promoted by the ECDS shall be conceived from the start for being capable of running in the cloud. The Cloud Strategy also encompasses a 'multi-cloud' aspect that will prevent the Commission from depending on one public cloud provider only. It is evident that the advantages of the cloud-first and cloud-native approaches will ultimately bring a high degree of flexibility in the Commission, giving it the option to choose the most suitable cloud provider based on the services needed.

In the wake of the Commission IT Security Strategy adopted in 2016, and in light of emerging new challenges related to IT Security worldwide, DIGIT has updated the Strategy and proposed a new rolling plan covering the period up to 2020. The **updated IT Security Strategy** – adopted by the ITCB in early 2019 – better defines DIGIT's role in delivering a number of measures to prevent and fight cyber-security related risks.

Concluding this series of strategic updates, DIGIT promoted in October 2019 the adoption of a Communication on '**the Workplace of the Future in the European Commission**⁹, endorsing a set of principles and recommendations aiming at strengthening the Commission's position as an attractive employer for highly qualified staff. Based on evidence and ideas gathered in a cross-cutting consultation process, the Communication proposes concrete measures to address the need to change working practices combined with the use of new technologies.

Following the appointment of President Von der Leyen, DIGIT was responsible for **providing adequate IT support during the entire process leading to the installation of the new College**, guaranteeing the smooth running of the necessary devices and infrastructure, with a group of DIGIT staff on permanent stand-by during the entire period from July until December 2019. This delicate yet fundamental moment of the Commission's lifecycle could run successfully thanks to an efficient, well-functioning IT environment. In this context, DIGIT also launched the development of the **eCollege, a highly secure and efficient information system** enabling a fully digitalised management of the College's weekly meetings, in line with the requirements of President Von der Leyen. Thanks to this new system, all relevant supporting documents (including sensitive ones) to be discussed at College level are available to the Commissioners directly on dedicated devices and without the need for any paper versions. The set-up of the **eCollege** (which started in August 2019 following a working agreement between DIGIT and SG, and currently continuing in an improvement phase) represents another important step towards the digital transformation as intended by the new political guidelines. The ultimate benefit is not just related to the fulfilment of one of President Von der Leyen's priorities: to establish a fully digital Commission that will lead by example vis a vis other European public administrations. The 'fully digital' approach will have a considerable impact on working methods and resource use, and highlights the Commission's strive to function as a green, efficient and modern administration. The advantage of the eCollege also translates into an improved efficiency of the decision-making cycle, while encompassing existing applications (e.g. Decide or Ares).

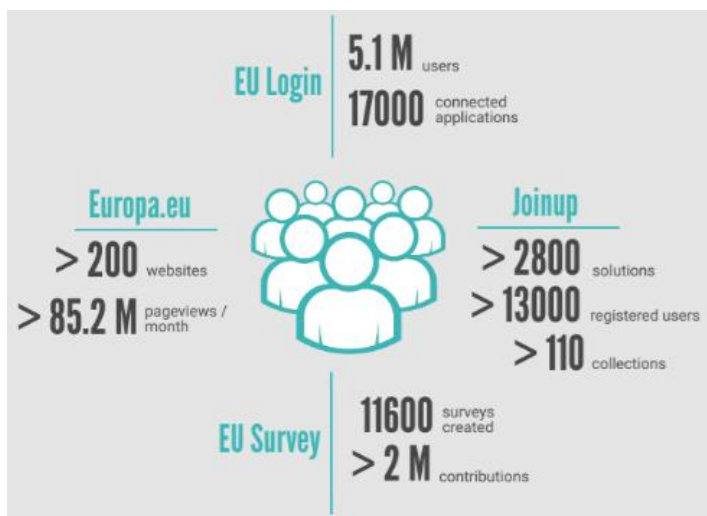
Delivering on 2019 Outputs

DIGIT's first priority focuses on the modernisation of public administration through a broad approach. Building on its mandate as leader of the ICT domain in the EU Commission, DIGIT has been pursuing the internal modernisation and digitalisation of the Commission's core processes (**Specific Objective #1**) over three dimensions: the **automation of core corporate processes**, the digital transformation enabled by **big data and data analytics solutions**, and the creation of a **Common Business**

⁸ https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en

⁹ C(2019)7450

Architecture. The three strands represent the pillars of the digital transformation agenda, finding their scope within the Synergies and Efficiencies Review in the ICT domain¹⁰. DIGIT's delivery under this domain has been mostly satisfactory and timely, and by year-end most of the outputs proposed in the 2019 Management Plan were fully delivered. As a result, new corporate solutions are available, with the Single Electronic Data Interchange Area (SEDIA¹¹), being one of the most successful examples within grant and procurement management as it allows suppliers to engage with the Commission in a purely digital way while simplifying, automating and hardening key processes such as approval, authorisation, payment, monitoring and fraud prevention. In addition, DIGIT continues enabling highly visible political initiatives through a solid partnership with other DGs. This is for instance the case with the WiFi4EU initiative that promotes free access to Wi-Fi connectivity for citizens. Concretely, after a first challenging phase in 2018, this project has now reached cruising speed and thousands of municipalities have, again this year, participated in an innovative first in/first out micro-grant call for tenders. The implementation of the **Data Strategy Action Plan** during the past year - following its endorsement by the Information Management Steering Board (IMSB) in 2018 - boosted DIGIT's role as provider of data analytics solutions and



services. The increased cooperation and knowledge sharing with other DGs enabled the collection of relevant information concerning stakeholder-specific problems and corporate requirements. As a result, DIGIT provided potential solutions tailored to the individual needs of its stakeholders, solutions that will represent elements of the offer of data and analytics services in the corporate data platform.

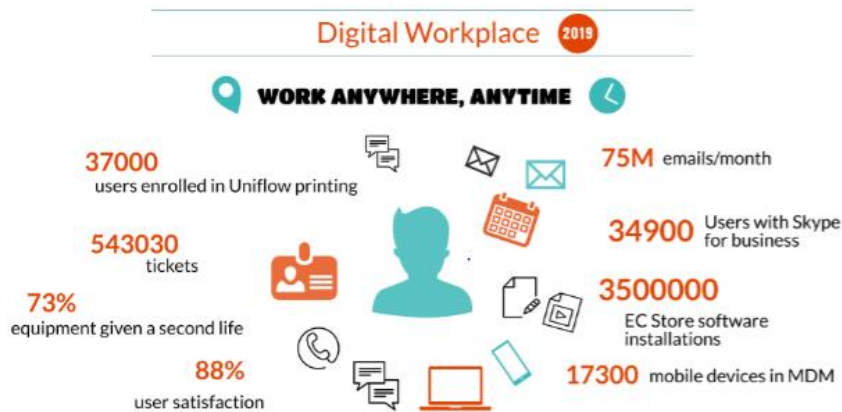
Considerable efforts were also dedicated to the **review of the**

Open Source Strategy. Following the establishment, back in 2000, of the first strategy for promoting the increased use of open source software in the Commission, DIGIT has completed a fourth review in order to address new emerging aspects, such as sharing, contributing and applying open source culture inside the European Commission. Although all the preparatory works and extensive research for the Strategy review were finalised in 2019 (including the launch of the inter-service consultation), the adoption process was delayed due to the need of synchronisation with the new Commission. The adoption of the Strategy is expected in the first half of 2020. Additionally, DIGIT continued the **development of interoperability solutions** as part of its responsibility for the ISA² programme, and further improved its offer of building blocks and digital services to Member States and other European stakeholders (**specific objective #2**).

The **Digital Workplace Programme (DWP)** is DIGIT's response to the need of **modernising office automation within the Commission (specific objective #3)**. Together with standardising and centralising management of end-user IT equipment and support services (**specific objective #4**), it underpins the digital workplace, DIGIT's second strategic goal.

¹⁰ [SER ICT](#)

¹¹SEDIA was replaced at the beginning of 2019 by the Funding & Tenders Portal (F&T), following a pilot launched in 2018 that proved the actual effectiveness of the electronic platform for grants and procurement contracts.



Previously framed as a pillar under the ICT domain of the synergies and efficiencies review, the Digital Workplace also plays a fundamental role in the new Digital Strategy, and consists of a combination of new tools, frameworks and working methods.

As part of this strand, the most successful outcome for 2019 is certainly the **transition from desktop to laptop**, resulting in 85% of Commission users having received a laptop largely exceeding the original target (initially set at 60%). End-users already equipped with corporate laptops could also exploit a new feature of the DWP, namely the **corporate Wi-Fi** available in Commission buildings in Brussels and Luxembourg. The extension of the corporate Wi-Fi happened gradually (covering only colleagues who already have corporate laptops with Windows 10). Since October 2019, many colleagues could already work 'on-the-go', remaining connected to the network and all their applications and files while being disconnected from the network cable. The extension is however still ongoing and will cover all EC office buildings by the second quarter of 2020. The positive impact of the DWP service offer is tangible: according to the 2019 IT Survey, **92% of the respondents found the IT service desk good or satisfactory**, a value that is way beyond the original target (maintain user satisfaction at least at 80%). As regards the **modernisation of data centre operations (specific objective #5)** and **consolidation of local data centres (specific objective #6)**, work advanced steadily with some exceptions due to the limited resources available (to dedicate to the consolidation process) in certain DGs.

To guarantee the smooth and secure running of the Commission's daily work, DIGIT delivers IT security processes and services, fulfilling the objective of **strengthening the Commission's cyber resilience (specific objective #7)** and **providing IT security operations (specific objective #8)**. The outputs planned for 2019 in these domains advanced as expected, and the establishment of the new College represented a new impulse to invest additional resources and efforts in cybersecurity. With over **50 presentations on cybersecurity** delivered during the year, and several tailored trainings and briefings targeting a diversified audience, DIGIT successfully achieved the original plan on cyber-awareness among the Commission staff.

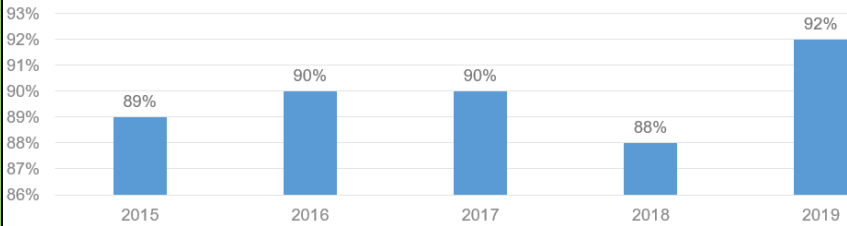
IT security operations facts



A **24/7 security operation capability** (in pilot since December 2019) has already been addressing IT security incidents occurring during Christmas holidays, although at present maintaining the required staffing level for ensuring the service remains a critical challenge. A well-established and properly functioning IT security governance framework also supports **better IT security decision making (specific objective #9)**. For this reason, in 2019 DIGIT developed and documented an IT Security Risk Management Methodology (ITSRM²) allowing system owners to identify, evaluate, document and treat IT-security risks.

The establishment of a Customer Relations Management is pivotal for understanding and addressing the needs of customers and end-users. For this purpose, following the creation of a dedicated and centralised CRM team, DIGIT invested more efforts on increasing customer focus by further enhancing the knowledge based activity. In this sense, the CRM team organised 45 sessions involving several DGs and services, with around 1.000 participants. The team engaged directly with customers from other DGs and EU Institutions both in Brussels and in Luxembourg through a range of initiatives aiming at understanding their business priorities, and to assist them with problems encountered with IT applications or Information Systems used. Leading the roadshows on the Digital Workplace and the benefits it brings to end users, was the key activity in 2019, aiming at changing the working culture of the Commission's staff. The activities running under this strand contribute to the overall achievement of the optimisation of DIGIT's delivery through the **increased customer focus (specific objective #10)** and **optimisation of resources management (specific objective #11)**.

b) Key Performance Indicators (KPIs)

| Result/Impact indicator | Trend | Target (or milestones) | Latest known results as per Annual Activity Report | | | | | | | | | | | | |
|--|------------------|---|--|------------------|------|-----|------|-----|------|-----|------|-----|------|-----|---------------------|
| KPI 1 The digital transformation composite index <i>Source: DIGIT</i> | 😊 | By 2020: Above 50% | <p>In 2019: 39.5%</p> <p>The forecast for 2020 sees an increase of the Digital Transformation Composite Index up to 54%. DIGIT considers this forecast as fully aligned with the target proposed in t Strategic Plan 2016-2020.</p> | | | | | | | | | | | | |
| KPI 2 Overall Satisfaction level of the end users with the digital workplace solutions provided by DIGIT <i>Source: DIGIT satisfaction survey on IT workplace solutions (2019)</i> | 😊 | <p>Maintain end user satisfaction at least at level of 80%</p> <p style="text-align: center;">Evolution of satisfaction for IT Helpdesk</p>  <table border="1"> <caption>Evolution of satisfaction for IT Helpdesk</caption> <thead> <tr> <th>Year</th> <th>Satisfaction (%)</th> </tr> </thead> <tbody> <tr> <td>2015</td> <td>89%</td> </tr> <tr> <td>2016</td> <td>90%</td> </tr> <tr> <td>2017</td> <td>90%</td> </tr> <tr> <td>2018</td> <td>88%</td> </tr> <tr> <td>2019</td> <td>92%</td> </tr> </tbody> </table> | Year | Satisfaction (%) | 2015 | 89% | 2016 | 90% | 2017 | 90% | 2018 | 88% | 2019 | 92% | <p>In 2019: 92%</p> |
| Year | Satisfaction (%) | | | | | | | | | | | | | | |
| 2015 | 89% | | | | | | | | | | | | | | |
| 2016 | 90% | | | | | | | | | | | | | | |
| 2017 | 90% | | | | | | | | | | | | | | |
| 2018 | 88% | | | | | | | | | | | | | | |
| 2019 | 92% | | | | | | | | | | | | | | |
| KPI 3 Consolidation level of data centres <i>Source: DIGIT</i> | 😊 | <p>By 2019:</p> <ul style="list-style-type: none"> - start¹² LDC consolidation activities for 80% of DGs; - Full consolidation of the DIGIT corporate data centre into two main sites (Betzdorf and Windhof). | <p>In 2019:</p> <ul style="list-style-type: none"> - consolidation started for 94% of all LDC - Betzdorf and Windhof have been consolidated and are operational | | | | | | | | | | | | |
| KPI 4 Level of IT Security Capability <i>Source: DIGIT</i> | 😊 | <p>By 2020: Achievement of level 3 or above (established, predictable or optimising) in the most critical processes and at least level 2 in the processes defined as core.</p> | <p>In 2019: Target met – detailed status with the breaking down of critical and core processes available under Specific Objective #7 in Annex 12 of this Annual Activity Report.</p> | | | | | | | | | | | | |
| KPI 5 Availability of a management system allowing flexible allocation of resources to priorities <i>Source: DIGIT</i> | 😊 | <p>By 2020: availability of a management system embedded in DIGIT's operations which:</p> <ul style="list-style-type: none"> - Allows flexible allocation of DIGIT's resources (staff and budget) to its priorities; - Is owned and used by DIGIT's management | <p>In 2019: All DIGIT activities consuming resources have been analysed across all directorates and documented in the first release of MAP. This decomposition underpins DIGIT's budget request for 2020 in view of the management priorities.</p> | | | | | | | | | | | | |
| KPI 6 Estimated residual error rate <i>Source: DIGIT AAR 2019</i> | 😊 | N/A | <p>Below materiality criteria of 2% (See AAR – Annex 4)</p> | | | | | | | | | | | | |

¹² This target was adjusted in the SER Communication adopted on 26/03/2019. Final consolidation of LDC will run beyond 2020 and will be completed by 2022.

c) Key conclusions on Financial management and internal control (executive summary of section 2.1)

In accordance with the governance arrangements of the European Commission, (the staff of) DG DIGIT conducts its operations in compliance with the applicable laws and regulations, working in an open and transparent manner and meeting the expected high level of professional and ethical standards.

To ensure the achievement of policy and management objectives, the Commission has adopted a set of internal control principles, based on international good practice. The financial regulation requires that the organisational structure and the internal control systems used to implement the budget be set up in accordance with these principles. DG DIGIT has assessed its internal control systems during the reporting year and has concluded that it is effective and the components and principles are present and functioning well overall, but some improvements are needed for Internal control principle 11 which is partially present. Please refer to AAR section 2.1.3 for further details.

In addition, DIGIT has systematically examined the available control results and indicators, including those for supervising entities to which it has entrusted budget implementation tasks, as well as the observations and recommendations issued by the internal auditor and the European Court of Auditors. These elements have been assessed to determine their impact on management's assurance about the achievement of the control objectives. Please refer to Section 2.1 for further details.

In conclusion, management has reasonable assurance that, overall, suitable controls are in place and working as intended; risks are being appropriately monitored and mitigated; and necessary improvements and reinforcements are being implemented. The Acting Director General, in his capacity as Authorising Officer by Delegation has signed the Declaration of Assurance.

d) Provision of information to the Commissioner(s)

In the context of the regular meetings between the DG and the Commissioner on management matters, the main elements of this report and assurance declaration, have been brought to the attention of Commissioner HAHN, responsible for Budget and Administration.

1. KEY RESULTS AND PROGRESS TOWARDS THE ACHIEVEMENT OF THE COMMISSION'S GENERAL OBJECTIVES AND DG'S SPECIFIC OBJECTIVES



In the 2016-2020 Strategic Planning and Programming cycle, DIGIT identified **11 Specific Objectives** contributing to the achievement of 2 General Objectives set at corporate level. The first one is “**to help achieve the overall political objectives, the Commission will effectively and efficiently manage and safeguard assets and resources, and attract and develop the best talents**”: it covers the horizontal nature and core actions that DIGIT implements as service provider across the Commission. However, DIGIT was also involved in the delivery of a policy objective, “a **Connected Digital Single**

Market”, by promoting the modernisation of the European public sector through the provision of interoperability solutions for European public administrations, businesses and citizens.

The eleven specific objectives are grouped under **five strategic priorities**, which provide additional steering in the long-term delivery process:

- **Modernisation of public administration**
- **Create the digital workplace of the future**
- **Create the data centre of the future**
- **Better IT Security**
- **Optimisation of DIGIT's delivery**

The following section provides an overview of the major achievements obtained by DIGIT while implementing the activities embedded in its Management Plan 2019. A thorough description of the complete list of activities is available in the Annex 12 to this Annual Activity Report.

1. MODERNISATION OF PUBLIC ADMINISTRATION

DIGIT's first priority focuses on the modernisation of public administration in a broad sense: internally, it concerns the **modernisation and digitalisation of the Commission's core corporate processes**, exploiting the power of new technologies and business models, and supporting the IT governance (**specific objective #1**). Until present, this strand also covered the SER digital transformation agenda through three dimensions: automation of core corporate processes, big data and data analytics solutions, architecture components.

The implementation of the digital transformation agenda proceeded according to plan, meeting most of the targets set in the Management Plan 2019.

- **Automation of core corporate processes:** simplification and automation of processes play a central role in the performance of an organisation. For this reason, DIGIT invested considerable efforts in this business area, in partnership with the other stakeholders concerned. The key deliverables – in this case – are linked to the provision of corporate digital services in the domain of grant management, eProcurement, eGrants, human resources, document management and legislative lifecycle management. The elaboration of customised workplans according to DG family facilitate the analysis and understanding of the different business needs, and consequently the identification of new initiatives and solutions. Among these, OPSYS was certainly one of the biggest achievement (it went live end of 2019). On the e-Procurement front, steady progress has been made with, for instance, the deployment of a new e-Submission module and the support of Framework contract with re-opening of competition. Due to the organisational, technical and business complexity of this ambitious program, some deliverables have nevertheless been postponed to 2020. In collaboration with the Secretariat-General, DIGIT also delivered the integration of the decision-making processes in Decide. A single workplace is now available for cabinets, as they can execute their approval tasks and follow-ups on ongoing Decisions files.
- **Big data and data analytics solutions:** The endorsement of the DataStrategy@EC Vision and Roadmap in 2018, and the related Action Plan, enabled DIGIT to consolidate its role in data analytics solutions and service provision, in close cooperation with other DGs in order to gather the necessary awareness on stakeholder-specific problems. Dedicated events, such as the Analytics and AI at the Commission, contributed too to raise awareness and gather requirements in this area. Thanks to this approach, and in line with the DataStrategy Action Plan, DIGIT already identified potential corporate solutions and tools. Consequently, the development of the data and analytics services pursued in line with the data platform development, in order to provide data and analytics services on top of the data platform infrastructure.
- **Architecture components:** the actions embedded under this strand in the Management Plan 2019 were oriented to the provision of digital solutions through a set of reusable building blocks. The ultimate goal is to drive reuse, enable common user experience, bring standardisation and reduce development costs. To this end, DIGIT started in 2019 the extension of the catalogue of reusable components, and elaborated a comprehensive software development platform, known as the Reusable Solutions Platform (RSP). The RSP is a portfolio of high quality, interoperable reusable solutions shaped as corporate management services. Concretely, the RSP provides business agnostic capabilities (e.g. authentication and identity management, search, document management, electronic signatures, etc.) while including in the platform a set of services that enable and facilitate the smooth integration of reusable solutions (i.e. support and advices, guidelines, reference implementations, etc). The ITCB approved the Project Charter and the Governance of the RSP in June 2019, and the platform portfolio already contains a good number of services that will increase according to their maturity level. An increasing number of projects make use of the RSP. In that context, the main challenge is to secure appropriate fundings to cope with the

growing demand and increase the number of Reusable Solutions as defined in the waves adopted at corporate level. In this context, Reusable Solutions from wave 2 and associated services are already available (EU Login, Search component, Hermes Repository Services, Corporate Notification Services, etc). As of 2021, it is expected that the co-financing mechanisms will provide a structural answer to this challenge.

The **review of the Open Source Strategy** represented another important step towards the modernisation process: with the first Strategy dating back to 2000 and having already gone through four reviews, the Commission has increased the use of open source software. The next step would be to address new parameters focusing more on sharing, contributing and applying open source culture inside the Commission, in order to acquire an 'inner sourcing'. Due to the transition towards the new Commission, the process leading to the adoption of the new Strategy (expected in December 2019) was slightly delayed, and the formal adoption will be formalised in 2020.

DIGIT's contribution to the modernisation of public administration also happens at external level, through the **provision of interoperability solutions (specific objective #2)**. At the core of this strand is the concept of interoperability, namely the "ability of organisations to interact and share information through the business processes they support by means of data exchange between their respective ICT systems". ISA² programme represents the executive arm that DIGIT uses to provide interoperable solutions across Europe, across different sectors and businesses. The **Connecting Europe Facility (CEF)** programme complements part of these actions, with DIGIT contributing through an offer of several building blocks and digital services (e.g. e-Invoicing, e-Procurement, e-Identity, e-Signature, e-Delivery).

In 2019, DIGIT continued to promote the modernisation of European Public Administrations based on the provision of interoperability solutions and Digital Single Market building blocks. Since January 2019, the merging of digital and interoperability checks allowed a better screening of the impact on ICT of major legislative proposals from the Commissions.



New proposals and evaluations published on the 'Have-your-say' Europa-webpage could already benefit from the interoperability checks methodology.

ISA² aims at promoting a holistic approach to interoperability in the EU, by identifying, creating and operating interoperability solutions and facilitating their reuse by European public administrations.

Following the adoption of the ISA² Work Programme in March 2019, DIGIT launched the **interim evaluation**, publishing the results in the form of a **report to the European Parliament and the Council¹³ of the EU** on 23 September 2019. The

report shows positive results on the overall performance of ISA² Programme, as

¹³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:615:FIN>

emerged after a number of consultation activities, including targeted interviews, online surveys, a public consultation and questionnaires distributed during several events. The interim evaluations also underlined that the main objectives of the Programme proved to be still pertinent and aligned with the results achieved. The stakeholders consultations, together with extensive desk review, also led to the identification of key-areas for improvement. This concerns the need 1) to raise more awareness beyond national administrations by fostering more collaboration and exchanges of views with regional and local administration¹⁴; 2) to move from user-centric to user-driven solutions; and - in the aftermath of the Programme's conclusion - 3) to pave the way towards an increased sustainability, in order to preserve and build on the achievements already obtained. Additionally, the results of the stakeholders consultations also showed that Member States should be more involved when it comes to the implementation of a more effective e-administration at national, regional and local level, as they are in a better position to complement the initiatives on interoperability and digitalisation entailed at EU-level. These results were based on data collected from 129 consulted stakeholders, 19 extensive desk research, and expert assessments.

The limited awareness of ISA2 and other initiatives related to interoperability, especially at the regional and local levels and the lack of coordination with ERDF funded solutions/systems, prevents the reuse of solutions. As conditionality is a very heavy and an extra burden on cohesion instruments, it was not taken on board, while the focus was in increasing awareness of the ISA² solutions and frameworks in the context of regional and local programmes. ISA² proved to be an appealing programme with new Countries showing interest in joining the Interoperability network in 2019. A good cooperation has been established with Japan –not yet formalised by an official agreement– and Albania has also expressed its interest in joining in.

While supporting the building of a **Digital Single Market**, DIGIT further enhanced the **reuse of Building Blocks**, fulfilling at the same time the 'Once Only Principle'. The figures of the latest report on the CEF-funded Digital Service Infrastructure (DSI, also known as 'building blocks') show that their adoption steadily increased during 2019. There are currently eight building blocks available, namely the Big Data Test Infrastructure, the Context Broker, Archiving, eDelivery, eID, eInvoicing, eSignature and eTranslation.

The graphic below embodied shows the evolution of the building blocks reuse from their introduction in 2014 until the second quarter of 2019.



¹⁴ In this respect, some consulted stakeholders pointed out existing synergies – and potential overlaps – with the European Regional Development Programme, which could serve as a starting point to reach regional public administrations more effectively in the future.

Evolution of reuse



2014 - Q2 2019, CEF Monitoring Dashboard

THE EU ADDED VALUE OF THE ISA² PROGRAMME

(Source: ISA² Interim Evaluation)

The implementation of the ISA² programme enabled – since the past 5 years – the delivery of interoperability solutions and digitalisation of public administrations across European borders, building on the achievements already obtained by its predecessor, the ISA programme.

The results of the Interim Evaluation provided a clear analysis on the overall perception of the European added value of the programme. Most of the stakeholders responding to the assessment highlighted how ISA² could achieve its objectives at a lower cost, when compared to the initiatives launched at national or sub-national level. Moreover, ISA² supported the growth of cross-border interoperability in the EU, raising awareness about interoperability across Member States, creating networks and facilitating exchanges. Synchronised with the implementation of the European Interoperability Framework (EIF), the programme further enhances the coordination of common EU policies under the digital single market.

2. THE DIGITAL WORKPLACE OF THE FUTURE

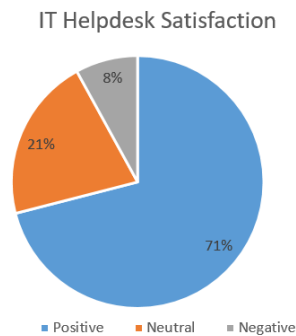
In line with the Digital Workplace Strategy (SER ICT), during 2019 DIGIT has worked on implementing and consolidating the six strands defined in the **Digital Workplace Programme: devices, office automation, email and calendaring, unified communication, collaboration and identity and access management**. On each of these dimensions, the delivery was satisfactory, as suggested by the following results:

- The transition from desktop to laptop, whose completion is expected by end 2020, advanced steadily. In December 2019, 85% of the EU Commission staff had a laptop.
- The improvement of mobile services progressed well. DIGIT just started a limited pilot for installing seamless Unified Communication (Skype for Business) on mobile devices.
- In terms of office automation, the roll-out of Windows 10 proceeded well during the first semester, and full migration of normal end users was completed by the end of 2019. At present, the upgrade concerned 37000 computers in the whole Commission. In order to ensure a better monitoring of the process, the upgrading of computers (and users) ready to migrate proceeded on a gradual basis. As a lesson learnt from the previous year's exercise, the roll-out of Unified Communication (UC) and the migration from legacy phones to UC telephony has been followed by regular communication with end users, including face-to-face trainings, demonstrations and presentations.
- 72% of the targeted population has now migrated from legacy phones to UC phones exceeding the initial target. This migration led end users to connect in an intuitive and automated way with internal and external users from anywhere, anytime and from any device. The transformation triggered by the introduction of Unified Communication solutions has ultimately the goal of establishing one central control layer that will route all services from the different application layers (for the time being, the existing infrastructure is composed by 3 main parts: classic telephony, Skype for business and videoconferencing).

There are no doubts on the positive impact of ICT services across the Commission, but a certain number of challenges remains. It is arguable that new ICT tools and methods often meet some initial resistance from end-users. In 2019, this was the case for the roll out of the **Unified Communication and Collaboration** (UCC) tools to the Commission Staff. Started in 2018, UCC software introduced a combined system of telephony, instant messaging, videoconferencing, sharing and collaboration capabilities through a single tool. Initially, the rollout proceeded at a slower pace than expected, but DIGIT responded by proactively establishing a communication campaign in order to better explain the change occurring in the advent of the UCC. These efforts determined the successful enrolment of all Commission users in UCC by June 2019, and proved to be a winning strategy when the Commission staff is facing significant changes in the working habits, such as the introduction of new IT tools.

DIGIT has been measuring the satisfaction level of the Commission's end users on the changes occurred in the Digital Workplace since 2016. The IT Survey 2019 showed how end-users satisfaction grew proportionally with the introduction of new IT tools, or important modifications in the digital workplace, following a transitory adaptation period when the modifications introduced (new printing system, upgrade to Windows 10, new Commission mobile apps, replacement of PCs) needed a certain 'acceptance time' from end-users. For 2019, the results of the IT Annual Survey on the end users' satisfaction with the IT Helpdesk show an increase over 2018. The overall satisfaction level of 92%, well-above the predefined target of 80%. It is proof that the actions implemented last year were effective and appreciated by end users. However, feedback from end-users indicate a continuous need to modernise our helpdesk service to reflect the changing needs of the Commission staff to work in a more efficient way. Over the past five years, the analysis of the end-users' satisfaction with the IT Helpdesk support highlights that it remained well-above 80%, with a slight drop in 2018 and a peak level of 92% in 2019. Reasons that explain the slight drop in 2018 are the better training needed for the Helpdesk consultants, longer hours of dedicated support and the easiness to connect with the same person that handled the incident first. A focus on enhanced and quicker communication on IT developments features high among the suggestions for further improvement. While there is a clear increase in the satisfaction level on almost all domains, some others, such as the use of the full potential of Unified Cooperation and Collaboration (Skype for Business) require a particular focus on further communication and training.

Satisfaction of EC Helpdesk services



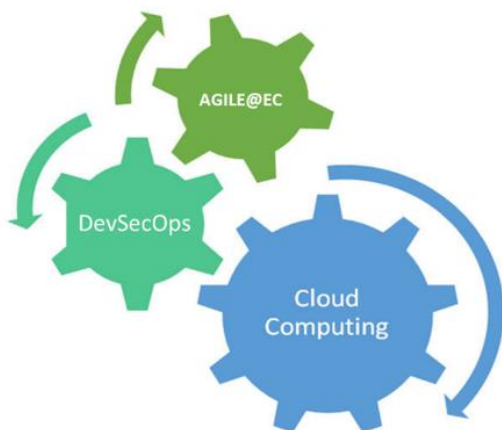
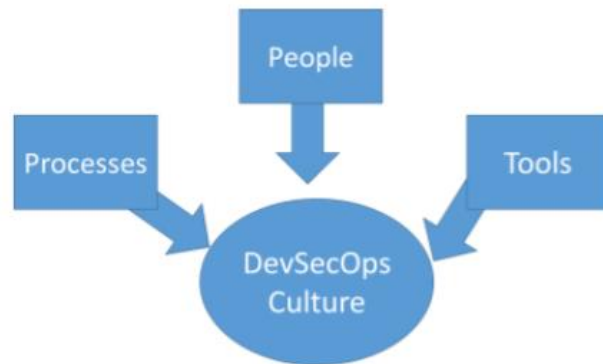
- 92% satisfaction ↑ from 88% last year
- Suggestions to improve:
 - Competency of Helpdesk consultants
 - Process improvements

3 THE DATA CENTRE OF THE FUTURE

DIGIT pursues the creation of the data centre of the future by **modernising the data centre operations towards hybrid cloud (specific objective #5)** and by **consolidating local data centres (specific objective #6)**. These objectives are ultimately linked to the effective and efficient management and safeguard of the Commission's assets and resources. In fact, the actions that DIGIT proposed so far in this context generated an overall improvement of reliability, security, agility, cost-efficiency and transparency of the ICT infrastructure service offering.

DIGIT advanced well with the implementation of the outputs fixed in 2019: the streamline of the **Cloud Broker Service** – aiming at providing Cloud resources and managing cloud contracts for the whole European Commission – enabled 12 Institutions and 33 customers DGs to exploit it. The financial volume purchased and managed by the cloud broker service on behalf of the participating stakeholders reached by year-end a total of 8 million euro, exceeding the initial target of 5 million euro set for 2019.

An increasingly important strand of the modernisation of data centre operations concerns the **DevSecOps**. An **enabler of the EC Digital Strategy**, DevSecOps is a philosophy, a cultural mind-set that combines multiple dimensions (development, security and operations) to make cultural transformation happen in both DIGIT and the Commission. Based on PM2 and agile methodologies, and exploiting the principles of the cloud native architecture, DevSecOps is influencing the way of developing and operating IT applications within the Commission, thus concerning Developers, Testers, Operation teams, security experts, analysts, portfolio managers and project managers. In 2019, DIGIT efforts focused on **building a DevSecOps community** through the organisation of conferences in Luxembourg and Brussels. Besides that, it also produced a 'development toolkit' that introduced new mechanisms enabling DevSecOps practices, as part of a standard offering of 'Service4Developers'.



A **new Cloud Strategy** based on the '**Cloud first approach**' - providing a more holistic approach with a broader spectrum than a mere governance strategy - has replaced the last EC Cloud Strategy, dating back to 4 years ago. The new setup represents an optimal combination between the advantages of a public cloud market with those linked to a secure private cloud on premise.

4 BETTER IT SECURITY

The provision of **better IT Security Services (specific objective #7)**, supported by the **provision of IT Security operations (specific objective #8)** emphasise prevention and focus on the development and deployment of IT security processes while improving the baseline IT Security of corporate infrastructure. The achievements of the targets set in 2019 are fully satisfactory, according to the evidence described below:

The main efforts in 2019 focused on ensuring a better level of security of the Commission IT infrastructure, as well as on secure development, operations and working methods concerning communication and information systems (CIS). We have successfully integrated the IT security risk management methodology (ITSRM²) with the elements of Data Protection Impact Assessments, reinforcing synergies between the two domains. In an increasingly client-centred approach, DIGIT focused on improving IT security services, standards, guidelines, training courses while boosting staff cybersecurity awareness and providing a secure working environment. The IT Security

Strategy is fully aligned with the principles and objectives of the European Commission Digital Strategy (ECDS), as well as with the current IT security Framework at the European Commission. DIGIT coordinated activities focused on development of both preventive and defensive measures.

In parallel, the progress reached on projects implementing the Digital Workplace, Cloud Strategy (private cloud on-premise) and HTTPS everywhere, contributed to an overall improvement of the global IT infrastructure security level.

In order to secure and protect the Commission's IT assets and resources, DIGIT builds, maintains and extends the activities of Security Assurance/Vulnerability Management, Security monitoring, Information Security Incident Management, Threat Hunting and Security Operations Engineering. In line with the planning, the 24/7 IT Security Response service was released on 5 December 2019 in pilot mode. It already proved its efficiency during the Christmas break, which is the most critical period as Commission offices are closed for one week. Thanks to the engagement of S2 team members, we managed to overcome the difficulties encountered to recruit adequate resources on the allocated AD posts. However, this best-effort approach is not sustainable. Efforts have now to be concentrated on the staffing to ensure the stability of the service. As proposed to the CMB, an assessment of the new 24/7 service is foreseen at the end of 2020 with the objective of verifying whether the chosen option (on-call) fits the Commission needs, or if the service would have to be adapted to on-site operational mode.

Complementary to specific objectives 7 and 8, the implementation of an **improved IT security decision making (specific objective #9)** ensured – since the past 5 years - an efficient IT security governance, while keeping senior management, IT experts and end-users informed about global IT security posture (risks and threats). Therefore, the related outputs focused on providing efficient support to the decision process, sharing of information and raising awareness on IT security matters.

For the achievement of this objective, covering the area of IT security risk management and reporting, DIGIT developed and documented the IT Security Risk Management Methodology (ITSRM²). The methodology allows system owners to identify, evaluate, document and treat IT-security risks at the level of the information systems that support the Commission business/policy processes. To ensure the highest degree of cooperation and inclusiveness across the Commission, DIGIT engaged with the LISO network and the system owners' community to disseminate the methodology and to assist in its practical application through dedicated coaching, training and support. The methodology has, since, been applied to a first set of information systems in DIGIT and in other DGs: to help the system owners perform the risk assessments and document the level of implementation of security controls for their information systems and to report centrally to the governance level on IT security risks. DIGIT prepared the first annual IT Security Risk Report, which was then adopted by ITCB. The report includes an action plan on IT security risk posture improvement indicating that throughout 2020 DIGIT will assist and support the DGs in its implementation.

The LISO centralisation project, started as a pilot in 2018, created a dedicated central team of ICT security experts within DIGIT S, the c-LISO team. The objective of the team is primarily to enhance the quality and efficiency of the Local Informatics Security Officer (LISO) function and provide better supervision, support and advice in the field of ICT security.

The pilot implementation of the service has been completed successfully in 2019 with 7 Commission departments: CNECT, DGT, DIGIT, NEAR, RTD, PMO and REA. The centralised pilot project received a very positive assessment by all participants through a satisfaction survey. In particular, the following benefits emerged:

- Greater professionalisation of the LISO function;
- More optimal usage and development of scarce skilled resources;
- Greater recognition, empowerment and career development perspective for the individuals;
- Assurance of service continuity;
- Enhanced maturity of the team organisation, processes and tooling;
- Increased cyber-security awareness and governance overall.

Consequently, there is the intention to plan a structured development of the service in the coming years (which already initiated by a call for expression of interest during the summer of 2019, with eight additional Commission departments positively replying to that call). The c-LISO team is therefore expected to extend its services from 7 to 15 Commission departments in 2020, serving entities that count for around 40% of the total IT end users within the Commission.

2. ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL

This section explains *how* the DG delivered the achievements described in the previous section. It is divided into two subsections.

The first subsection reports the control results and other relevant information that support management's assurance on the achievement of the financial management and internal control objectives¹⁵. It includes any additional information necessary to establish that the available evidence is reliable, complete and comprehensive. It covers all activities, programmes and management modes relevant to the DG.

The second subsection deals with the other components of organisational management: human resources, better regulation principles, information management and external communication.

2.1 Financial management and internal control

Assurance is an objective examination of evidence for the purpose of providing an assessment of the effectiveness of risk management, control and governance processes.

This examination is carried out by management, who monitors the functioning of the internal control systems on a continuous basis, and by internal and external auditors. Its results are explicitly documented and reported to the Director-General. The reports produced are:

- the reports by AOSDs;
- the reports from Authorising Officers in other DGs managing budget appropriations in (cross) sub-delegation;
- the contribution by the Director in charge of Risk Management and Internal Control Coordinator, including the results of internal control monitoring at the DG level;
- the reports on recorded exceptions, non-compliance events and any cases of 'confirmation of instructions' (Art 92.3 FR);
- the reports of the ex-post exercise and of the audits performed;
- the limited conclusion of the Internal Auditor on the state of internal control, and the observations and recommendations reported by the Internal Audit Service (IAS);
- the observations and the recommendations reported by the European Court of Auditors (ECA).

These reports result from a systematic analysis of the evidence available. This approach provides sufficient guarantees as to the completeness and reliability of the information reported and covers fully the budget delegated to the Director-General of DIGIT.

This section is for reporting the control results and other relevant elements that support






¹⁵ Art 36.2 FR: a) effectiveness, efficiency and economy of operations; b) reliability of reporting; c) safeguarding of assets and information; d) prevention, detection, correction and follow-up of fraud and irregularities; and e) adequate management of risks relating to the legality and regularity of underlying transactions

management's assurance. It is structured into (a) Control results, (b) Audit observations and recommendations, (c) Effectiveness of internal control systems, and resulting in (d) Conclusions on the assurance.

2.1.1 Control results

This section is for reporting and assessing the elements identified by management which support the assurance on the achievement of the internal control objectives¹⁶. The DG's assurance building and materiality criteria are outlined in AAR Annex 4. Annex 5 outlines the main risks together with the control processes to mitigate them and the indicators used to measure the performance of the relevant control systems. It refers to the resources managed by DIGIT: Procurement and Revenues (charge back services) in 2019.

Coverage of the Internal Control Objectives

| Results | | |
|---------------------------------------|--|---|
| Legality & regularity | Residual error rate below 2% |  |
| Cost-Effectiveness of controls | Ratios cost-effective |  |
| Anti-Fraud Strategy | No qualification to the Declaration of Assurance |  |
| Safeguarding of assets | Assets safeguarded |  |
| Reliability of reporting | No material error and no reservations |  |

¹⁶ 1) Effectiveness, efficiency and economy of operations; 2) *reliability of reporting*; 3) *safeguarding of assets and information*; 4) prevention, detection, correction and follow-up of fraud and irregularities; and 5) adequate management of the risks relating to the legality and regularity of the underlying transactions, taking into account the multiannual character of programmes as well as the nature of the payments (FR Art 36.2). *The 2nd and/or 3rd Internal Control Objective(s) (ICO) only when applicable, given the DG's activities.*

A. Procurement

The intrinsic risk for the expenditure managed by DIGIT including procurement is considered relatively low because of the centralised and direct mode of budget implementation. The Relevant Control System for Procurement (annex 5) demonstrates how the control systems in place in the DG address the risks.

1. Effectiveness

❖ *Legality and regularity of the transactions*

DIGIT has set up internal control processes aimed to ensure the adequate management of the risks relating to the legality and regularity of the underlying transactions, taking into account the multiannual character of programmes as well as the nature of the payments concerned.

The objective is to ensure that the DG has reasonable assurance that the total amount of any financial operation authorised during the reporting year which would not be in conformity with the applicable contractual or regulatory provisions does not exceed 2 % of the total expenditure (see annex 4 - Materiality criteria). During 2019, six procurement procedures were launched for a total value of EUR 814 750 398.

| Procedure Legal base | Number of Procedures | Amount (€) | Representing ... % of total value |
|---|----------------------|----------------------|-----------------------------------|
| Negotiated procedure without prior publication (Annex 1 - 11.1) | 4 | 288 360 618 € | 35% |
| Open procedure (FR 164 (1)(a)) | 1 | 108 666 493 € | 13% |
| Restricted procedure with Dynamic purchasing system (FR 164 (1)(b)) | 1 | 417 723 287 € | 51% |
| | 6 | 814 750 398 € | |

The procurement needs were thoroughly defined and planned (operationally and economically). DIGIT Procurement Board chaired by the Director General discussed and approved the related procurement procedures (EUR 144 000 or above). Additionally, AO(S)D validated all planned procurement procedures before launching the process. During the year, no planned procurement procedure was cancelled.

During the procurement process, the exclusion criteria are applied and well documented; EDES is checked. Furthermore, once at award phase, most procurement procedures are communicated to the GAMA (Groupe d'Analyse des Marchés) which after a risk-based assessment selects some procurement procedures for examination. This risk assessment relies on a combination of three criteria: type of procedure, number of offers received and financial volume of the awarded market. Given that GAMA performs the risk-assessment and examination of the procurement process as an external (neutral) and independent body, its opinion is highly valued by both IAS and ECA.

The benefits of the controls in place at planning and validation phase, though not quantifiable, are numerous and effective: better value for money, deterrent effect, efficiency gains, system improvements, compliance with regulatory provisions. They also limit litigation risks and risks of cancellation of a tender, as shown by the zero valid complaints and litigation cases received.

| | Amount | Number |
|-------------------------|-----------------------------|----------------------|
| Commitments made | € 332 218 317 | 4668 |
| Payments made | € 327 101 160 | 9035 |
| <u>Total</u> | <u>€ 659 319 477</u> | <u>13 703</u> |

The total amount of 2019 commitment appropriations represents EUR 332 218 317, the execution rate of these appropriations for 2019 is 97.66% which represents EUR 327 101 160, the remaining appropriations will be executed in 2020. The authorised payment appropriations, including the amounts carried over from 2018, represent EUR 433 303 185. Payments made during the financial year amounted to EUR 327 101 160 which represents an execution rate of 75.5 %.

During 2019, a total of 9035 payments were made, amounting to EUR 327 101 160. 97.4 % of these payments were made on time, with an average payment deadline of 13.7 days. 454 payments were suspended for an average suspension period of 27 days. An amount of EUR 19 396 was paid as interest due to late payment, representing only 0.006% of total amount paid.

Ex-ante controls have been performed on 100% of payments, in order to detect and correct any procedural errors with or without financial impact. This has allowed payments to be free of financial material error. The majority of errors detected (ex-ante) was of a procedural nature and corrected before payment. This confirms the strong deterrent effect that ex-ante controls have on financial transactions.

Out of the 537 recovery orders sent out in 2019, only 1 concerned recovery of payments or late interest penalties for an amount of EUR 19 492 (representing 0.006% of the payments made). The other 536 recovery orders concerned chargeback (see page xx).

Following re-engineering of the financial management process in 2016, DIGIT's senior management decided to decentralise the function of AOSD for commitments. In 2019, 100% of the 4668 commitments were submitted to ex-ante controls in order to detect and correct any procedural errors with or without financial impact. The operational units are responsible for the operational initiation and verification of commitments. The finance unit performs the financial initiation and verification, it ensures the creation of the budgetary commitment and the signature process for specific contracts. 100% of commitments and contracts undergo ex-ante controls before the signature. The finance unit also ensures that the contract execution is "certified correct" which is provided by the operational units ; 100% of payments undergo ex-ante control.

During the reporting year, there were 195 recorded non-compliance events, with however zero impact on the legality and regularity of the transactions. Apart from technical or procedural errors, these events mostly concerned '*saisine a posteriori*'. Most of them consisted of 2019 budgeted expenditures corrected during the same financial year; this is a formal compliance issue that does not have a negative impact on the budget. Furthermore, all non-compliance events concerned expenditures that were foreseen, budgeted and covered work duly performed, therefore due.

Also, 17 exception events were recorded. 16 of these events concern the non-respect of the annuality principle, contracting was done in 2019 on 2019 budget but the execution of the contract will only start in 2020. The main reason for this is that it was not possible to complete the 2019 work plan for some sectors. This for several reasons including a

shortage of experts (some experts were recruited late in the year 2019), the complexity of the work at hand or the necessity to execute additional urgent work. The budget is co-delegated and made available in a piece meal manner and in some cases depends on the approval/discussion in Steering Committee meetings that are typically planned in Q3 and Q4 of the year. To increase the predictability of the availability of appropriations DIGIT should agree with stakeholders to make 80% of the budget available in Q1 and the remainder in Q3. Discussions with the other DGs have started. Closer monitoring of the budget execution to further improve cooperation within DIGIT with relevant services including e.g. to invite the contract cell to regularly attend meetings and work closely on budget planning and execution.

The other exception report concerned the recourse to a negotiated procedure without prior publication for extreme urgency reasons.

A first analysis of the typology of 2019 non-compliance and exception events seems to indicate that the same problems persist from previous years, despite the actions already taken in 2019 such as the review and strengthening of the procedure.

Indeed:

- ✓ 41 % of non-compliance events relate to the late renewal of software licenses or maintenance of those licenses,
- ✓ 17 % relate to the late renewal of Specific Contracts for External Service Providers
- ✓ 11 % relate to the late renewal of hardware maintenance contracts
- ✓ The remaining 31 % concerned a variety of other issues. Mainly these issues concerned the annuality principle, contracts were signed in 2019 but work will be carried out in 2020.

One atypical issue included under a "variety of other issues", relates to the authorisation of payments by two members of the finance team, without being covered by a sub-delegation act. Those two persons were however:

- duly appointed as Financial Verifying Agent (FVA) and Authorizing Officer by Sub-delegation (AOSD)
- provided with the "Code of professional standards for staff responsible for financial verification" for FVA
- provided with the Charter for AOSD end 2018 (and they signed it)
- granted AOSD access rights

The step of the sub-delegation act, normally linked to the signature of the Charter was missed.

As soon as the issue was discovered during ECAs annual control of transactions, the sub-delegation act for one of the concerned staff was immediately launched and signed. The other staff member had in the meantime left DIGIT. A non-compliance event was then added to the register, with the list of payments at stake.

This event is not considered as a structural weakness in the control systems in place, but rather as a missed step in a well-defined process (human error). The access rights and related obligations are subject to a periodic monitoring twice a year. For one of the staff members, the period as FVA/AOSD lasted 3 months, unfortunately this happened between the two yearly controls. When this case was detected, the second yearly monitoring (initially foreseen for end of 2019) was immediately performed and spotted the second case. Reinforced mitigating measures have now been put in place by the unit in charge to avoid similar situations in the future and ensure full compliance with Article 7 of the Internal rules.

Further actions will be taken in 2020 with the objective of further raising awareness and following up of outstanding issues, quarterly reporting to Senior Management will continue.

In conclusion, the analysis of the available control results, the assessment of the weaknesses identified and their relative impact on legality and regularity has revealed no significant weakness that could have a material impact as regards the legality and regularity of the financial operations. Consequently, the control objective as regards legality and regularity has been achieved.

In the context of the protection of the EU budget, at the Commission's corporate level, the DGs' estimated overall amounts at risk and their estimated future corrections are consolidated.

Over the past years, the implementation of ex-ante and ex-post controls has not resulted in any major financial correction/recovery order after payment. This is due to the fact that no financial error has been detected and administrative errors were corrected before payments were made. These results are expected to continue, having as a result an estimated future financial corrections (0.0%)¹⁷.

Yet, in order to avoid any potential underestimation, DIGIT calculates, in accordance to central services guidance on the content of the AAR, the Most Likely Error (MLE) for the Commission's administrative expenditure (0.50%) as a conservative estimate in order to allow the consolidation of data when determining the amount at risk at payment at Commission level. This percentage corresponds to an estimated overall amount at risk at closure of EUR 1 635 506.

This is the AOD's best, conservative estimation of the amount of relevant expenditure during the year (EUR 327 101 160) not in conformity with the applicable contractual and regulatory provisions at the time the payment is made. For DIGIT, the estimated overall amount at risk at closure equals the estimated overall amount at risk at payment since there is no expectation of any future financial correction.

¹⁷ It should be noted that out of the 537 recovery orders sent out in 2019, only 1 concerned recovery of payments or late interest penalties for an amount of EUR 19 492. The other 536 recovery orders concerned chargeback; therefore we have adjusted the ARC from 0.1% to 0.0%.

Table - Estimated overall amount at risk at closure

| DIGIT | 'payments made' (FY; m€) | minus new ^a prefinancing | plus cleared prefinancing | "=Relevant expenditure" | Average Error Rate (weighted AER; %) | estimated overall amount at risk at payment (FY; €) | Average Recoveries and Corrections (adjusted ARC; %) | estimated future corrections | estimated overall amount at risk at closure ^e (€) |
|-------|-----------------------------|---|---|-------------------------|---|---|--|------------------------------|--|
| | | | | (for the FY) | | | | [and deductions] (for FY; €) | |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) |
| | as per AAR annex 3, table 2 | as per ABAC DWH BO report on prefinancing | as per ABAC DWH BO report on prefinancing | = (2) - (3) + (4) | Detected error rates, or equivalent estimates | = (5) x (6) | H-ARC (as per ABAC DWH BO report on corrective capacity), but adjusted | = (5) x (8) | = (7) - (9) |
| | 327 101 160 € | 0 € | 0 € | 327 101 160 € | 0,5% | 1 635 506 € | 0.0% | 0 € | 1 635 506 € |

(1) differentiated for the relevant portfolio segments at a level which is lower than the DG total

(2) Payments made or equivalent, e.g. expenditure registered in the Commission's accounting system, accepted expenditure or cleared pre-financing. In any case, this means after the preventive (ex-ante) control measures have already been implemented earlier in the cycle. In all cases of Co-Delegations (Internal Rules Article 3), "payments made" are covered by the Delegated DGs. For Cross-SubDelegations (Internal Rules Article 12), they remain with the Delegating DGs.

(3) New pre-financing actually paid by out the department itself during the financial year (i.e. excluding any pre-financing received as a transfer from another department). "Pre-financing" is covered as in the context of note 2.5.1 to the Commission annual accounts (i.e. excluding "Other advances to Member States" (note 2.5.2) which is covered on a purely payment-made basis). "Pre-financing paid/cleared" are always covered by the Delegated DGs, even for Cross-SubDelegations.

* In Cohesion, the (10%) retention made.

(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').

* In Cohesion, the retention which is now released 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, and adds the previous pre-financing actually cleared 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 order to calculate the weighted Average Error Rate (AER) for the total relevant expenditure in the reporting year, the detected error rates have been used – or an equivalent. 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 subsidies to agencies), it is nevertheless recommended that 0.5% be used as a conservative estimate.

(8) Even though to some extent based on the 7 years historic Average of Recoveries and financial Corrections (ARC), which is the best available indication of the corrective capacity of the ex-post control systems implemented by the DG over the past years, the AOD has adjusted this historic average from 0,3% to 0%. It should be noted that out of the 537 recovery orders sent out in 2019, only 1 concerned recovery of payments or late interest penalties for an amount of EUR 19 492. The other 536 recovery orders concerned chargeback.

(10) 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.

Fraud prevention, detection and correction

DIGIT has developed and implemented its own anti-fraud strategy since 2013, elaborated on the basis of the methodology provided by OLAF at that time. It is updated every 3 years or more often should circumstances require it. It was last updated in 2017. The strategy covers the inherent risks derived from the main activities of DIGIT and builds on the mitigating measures currently in place. In this context, a number of actions were defined and implemented during 2019, which aimed to achieve the set objectives:

- ✓ as in previous years DIGIT, assessed the risk of fraud in the context of its risk management exercise
- ✓ in October 2019, the Director General raised awareness of all statutory staff and issued "Guidelines for meetings with private companies". It details principles framing these meetings, and provides pointers to the relevant documents or provisions.
- ✓ During the reporting year, OLAF has not initiated any case, which concerns the activities of DIGIT.

DIGIT is lead DG for one item of the action plan of the new Commission Anti-fraud Strategy (CAFS): *"Regularly revise and update the corporate IT security strategy and monitor its implementation. Optimise the systems of the Commission and the executive agencies for secure operation of e-procurement, e-grants and other channels of e-governance."* The target date set for the implementation of the action is "continuous".

Following the bi-annual review cycle, the updated version of the IT Security Strategy and the accompanying Action Plan were adopted by the IT and Cybersecurity Board (ITCB) on 14 February 2019. The progress of the implementation of the strategy is monitored and the corresponding status updates and reports are provided to DIGIT IT Security Board (DISB) and to the ITCB on a regular basis.

In the comprehensive approach to IT security, in June 2019 DIGIT released the guidelines on IT Security in System Life-Cycle, providing a global view on the security processes required to develop and operate appropriately protected IT systems, from their inception to their decommissioning. The guidelines provide references to specific parts of the IT security policy framework (Commission decision 2017/46, its implementing rules and the corresponding standards), methodologies and operational services that have been put in place and are continuously developed, under the mandate of DIGIT, in order to support the System Owners in the implementation of the IT security principles and in applying security controls allowing to mitigate identified risks.

DIGIT plans to revise its anti-fraud strategy in 2020 to take into account the new Commission Anti-Fraud Strategy adopted in 2019, and take advantage of the enhanced support offered by OLAF, for example regarding fraud-awareness trainings/actions. DIGIT new AFS will elaborate on the latest measures taken and if needed adapt the related action plan, to include for instance DIGIT contribution to the CAFS action plan mentioned above. Following the adoption of DIGIT new AFS, an awareness raising action will be conducted within the DG.

DIGIT overall exposure to fraud is low (no OLAF case) and mitigating measures are in place to mitigate the existing risks. Therefore, the residual risks for all types of fraud remain very low. DIGIT considers that its fraud prevention and

detection strategy is working well and that DIGIT collaborates to the Commission Anti-Fraud Strategy action plan in a relevant manner.

Budget implementation tasks entrusted to other DGs and entities

This section reports and assesses the elements that support the assurance on the achievement of the internal control objectives as regards the results of the DG’s supervisory controls on the budget implementation tasks carried out by other Commission DGs and entrusted entities distinct from the Commission.

DIGIT grants cross-delegations for actions managed by other Commission services in the framework of the ISA and ISA² program. In 2019 DIGIT granted one cross-sub-delegations, on which EUR 11 250 were committed during 2019 and EUR 11 250 payments were made, to other services in this framework. In Commission services, the AOD is required to implement the appropriations subject to same rules, responsibilities and accountability arrangements. The sub-cross-delegation agreement requires the AOD of the relevant DGs and Services to report on the use of these appropriations. In their report, the AODs did not communicate any events, control results or issues which could have a material impact on the assurance.

2. Efficiency

The principle of efficiency concerns the best relationship between resources employed and results achieved. The principle of economy requires that the resources used by the institution in the pursuit of its activities shall be made available in due time, in appropriate quantity and quality and at the best price.

During 2019, a total of 9035 payments were made, amounting to EUR 327 101 160. 97.4 % of these payments were made on time, with an average payment deadline of 13.7 days. This indicator has remained quite stable over the years.

| | 2017 | 2018 | 2019 |
|----------------------------------|-------|-------|-------|
| % Payments made on time | 98.5% | 98.5% | 97.4% |
| Average payment deadlines | 13.5 | 12.9 | 13.7 |

3. Economy

DIGIT has made an estimation of the costs of the three main control phases: procurement, financial transactions¹⁸ and ex-post supervisory measures. Benefits of those controls have also been identified. When possible they have been quantified. In some other cases, benefits have been expressed through the corresponding relevant non-quantifiable indicator. The criteria for the calculation and the indicators used to assess the efficiency of controls are shown in the Relevant Control Systems in annex 5.

The total value of the **procurement** for 2019 is EUR 814 750 398 which represents a major decrease as compared to last year as no major Framework contract was renewed.

¹⁸ This includes committing and paying of appropriations

| | 2016 | 2017 | 2018 | 2019 |
|---|---|---|--|---|
| Value procurement | EUR 770 287 070 | EUR 1 214 411 872 | EUR 3 012 876 790 | EUR 814 750 398 |
| Increase / decrease of value in% | - | 57.7% | 148.1% | -73% |
| Cost of control (ex ante) | EUR 1 888 460 (0.25% on total value) | EUR 1 711 984 (0.14% on total value) | EUR 1 400 260 (0.046% on total value) | EUR 1 427 730 (0.18% on total value) |
| Cost per procurement procedure | EUR 157 372 | EUR 142 665 | EUR 155 584 | EUR 237 955 |

The procurement procedures are to a large extent a regulatory requirement which cannot be curtailed, difficulties linked to the type and complexities of each contract have to be taken into account. DIGIT's procurements serve the entire Commission as well as other EU Institutions and Bodies (regulatory agencies, joint undertakings). Considering the complexity of the procurement activities and the wide range of participants, the controls implemented are necessary and cannot be reduced as a significant proportion of the appropriations would be at risk if they would not be in place (as outlined in Annex 5).

For procurements, an estimated EUR 1 427 730 was invested in controlling (ex-ante) six procurement procedures for a total value of EUR 814 750 398 in 2019. Thus 0.18 % of the total contract value was dedicated to ex-ante control and each procurement procedure had an estimated cost of EUR 237 955. Compared to last year, this represents an increase (0.046 % in 2018) of the proportion of the total contract value dedicated to control but as mentioned in last year's AAR 2018 was an exceptional year due to the high value in procurement related to the renewal of 2 major Framework contracts.

DIGIT considers that the need of these controls is undeniable, as the totality of the procurements granted and appropriations would be at risk in case they would not be in place. The non-quantifiable (n.q) benefits of controls are identified in the corresponding Relevant Control System in annex 5 for each stage. In particular, the following good practices in relation to high value procurement procedures were identified by the IAS as a good practice during its Audit on Procurement:

- Preparation of appropriate strategy papers before the procedure is launched. These take into account the lessons learned from previous contract(s) and the analysis of the different procurement options that exist on the market for acquiring the goods/service needed;
- debriefing meetings with unsuccessful tenderers, aimed at obtaining feedback in order to consider any suggestions for improvement for future procurement procedures. In addition, DIGIT sends letters to potential contractors, inquiring as to why they did not participate;
- DIGIT's Procurement Board ensures that the procurement strategy is followed. The Board also monitors the implementation of the high value procurement procedures at different key stages (Orientation Document and Evaluation report).

DIGIT controls financial transactions as a whole from committing to paying the amount. Therefore, both commitments and payments made are calculated in the cost of control. EUR 235,5 is the cost per transaction, EUR 3 226 940 is the cost of control which represents 0,49% of the value transactions made. The cost per transaction has decreased with 8.5 % in comparison to last year (EUR 256 in 2018) while the amount of financial transactions has increased with 4%.

| 2019 | Amount | Number | Cost of control | In % of total value | Cost per transaction |
|-------------------------|-------------------------------|----------------------|-----------------------------|---------------------|-------------------------|
| Commitments made | EUR 332 218 317 | 4668 | EUR 1 688 250 | 0.51% | EUR 362 |
| Payments made | EUR 327 101 160 | 9035 | EUR 1 538 690 | 0.47% | EUR 170 |
| <u>Total</u> | <u>EUR 659 319 477</u> | <u>13 703</u> | <u>EUR 3 226 940</u> | <u>0.49%</u> | <u>EUR 235,5</u> |

DIGIT revised its ex-post control methodology (as also foreseen in the action plan of the 2017 Audit on procurement); it offers the possibility to perform specific ex-post control exercises based on the issues detected by the ex-ante control and/or during the IAS/ECA audits. It can also take into account the risk of fraud and other risk factors.

For the 2019 ex-post control exercise, a total amount of EUR 17 806 457 was verified which represents 5.4 % of the total of payments made in 2019. The amount controlled last year was EUR 8 509 304, which represented 2.82% of the total amount paid, thus the amount controlled increased with 109% this year. An estimated EUR 10 940 were invested (a decrease of 35% compared to last year's EUR 16 790) in controlling 15 payments for a total value of EUR 17 806 457. The cost per control is EUR 729 which is a decrease of 30% compared to the cost of last year's EUR 1049.

4. Conclusion on the cost-effectiveness of controls

Based on the most relevant key indicators and control results, DIGIT has assessed the effectiveness, efficiency and economy of its control system and reached a positive conclusion on the cost-effectiveness of the controls for which it is responsible.

DIGIT has made an estimation of the costs of the three main control processes on Procurement and administrative expenditure: Procurement, financial transactions and ex- post supervisory measures. Benefits of those controls have also been identified. When possible they have been quantified. In some other cases, benefits have been expressed through the corresponding relevant non-quantifiable indicator.

The costs of ex-ante controls performed by the DG on the procurement represent 0.18% of the total value of procurement made in 2019. The costs of ex-ante controls performed by the DG on the verification of financial transactions represent 0.47% of payments made in 2019 or 0.49% on all financial transactions made, seeing that DIGIT controls commitments and payments. Cost of controls of ex-post verifications represent 0.003% of payments made in 2019 and 0.06% of the amount checked ex-post. All controls performed are considered reasonable and have allowed to comply with the legality and regularity control

objective as detailed in the previous sections, i.e. 97.4 % of payments made on time, time to pay far below the maximum allowed of 30 days (13.7 days for 2019) and no relevant deficiencies detected by ex post controls.

In addition, it should be highlighted that there are a number of non-quantifiable benefits resulting from the controls operated during the implementation of DIGIT'S expenditure. These benefits are mainly to ensure compliance with relevant regulatory provisions and internal rules, to have a strong deterrent effect, to improve existing procedures and to avoid possible litigation and reputational risks. DIGIT considers that the need of these controls is undeniable, as the totality of the procurements granted and appropriations management would be at risk were they not in place. The non-quantifiable (n.q) benefits of controls are identified in the corresponding Relevant Control System in Annex 5 for each stage.

| | Amount | Cost of control | In % of related value |
|------------------|--------------------------|----------------------|-----------------------|
| EX ANTE 1 | EUR 814 750 398 | EUR 1 427 730 | 0.18% |
| EX ANTE 2 | EUR 659 319 477 | EUR 3 226 940 | 0.49% |
| EX POST | EUR 17 806 457 | EUR 10 940 | 0.06% |
| TOTALS | EUR 1 491 876 333 | EUR 4 584 315 | 0.31% |

The conclusion of the evaluation of costs and benefits of controls performed for the management of procurement and of the indicators used to measure their efficiency is that controls performed in DIGIT during 2019 have been cost-effective as the estimated benefits well exceeded the estimated costs, which are considered reasonable compared to the funds managed. Also the results of controls show the efficiency of those since they served to comply with the deadlines and mitigate the risks that they address. Thus the conclusion is that the applied control strategy is the best suited to fulfil the intended control objectives efficiently and at a reasonable cost and that it should remain unchanged.

B. Revenues (charge back services)

1. Effectiveness

The revenues of DIGIT concern services provided internally to other Commission departments and services, and those provided externally to other institutions, agencies and bodies. This process consists essentially of a series of sub-processes such as delivery of services, cost calculation and charge back.

To steer and control the process, a common framework has been set up, inspired by the following principles:

- The obligation to provide the services equally to all clients in terms of quality, timing and deliverables
- 'No-Profit': the provision of services should not result in a surplus
- Administrative cost-efficiency: the administrative costs resulting from the management of the process should be kept to the minimum.
- The modalities of the provision of services offered in the catalogue shall be agreed by the parties in a Service Level Agreement (SLA) or Memorandum of Understanding (MoU).

For services provided by DIGIT to other Commission departments and services (Internal), the preferred financial mechanism is to make the appropriations available through the horizontal co-delegation type II. It allows for simple and timely access to the resources and ensures a clear and direct accountability line for the management of the expenditure. The co-delegation mechanism requires a prior written agreement between the two services.

Responsibility for the use of budget appropriations remains with the AOD of the client. The co-delegation must be foreseen in Annex I to the Internal Rules.

For services provided by DIGIT to other EU institutions, agencies and bodies (External), the arrangements agreed must aim to ensure transparency and predictability in the use of resources, namely by making budget forecasts available on time and avoiding sudden and substantive price revisions. The authorising officers of all EU institutions, agencies and bodies involved remain accountable for the implementation of the actions and appropriations for which they are responsible under the cost recovery process in accordance with existing rules. As a rule, the funds recovered will be earmarked as assigned revenue on the budget lines of the Commission initially supporting the costs.

In 2019, DIGIT collected a total amount of EUR 156 571 817 of charge back of services.

| | Amount¹⁹ |
|---|-------------------------------|
| Charge back of services (Internal - collected through co-delegations) | EUR 115 620 374 |
| Charge back of services (External - collected through Recovery Orders) | EUR 20 701 477 |
| Charge back of services (Internal - collected through Recovery Orders) | EUR 20 249 966 |
| Total | <u>EUR 156 571 817</u> |

2. Efficiency

Besides the quantifiable benefits, more importantly in the current context of limited administrative appropriations, it is the non-quantifiable (n.q) benefits of the controls that are of particular importance :

- ✓ The pooling of resources in order to achieve better services at a lesser cost.
- ✓ Efficiency as know-how, capacities and resources developed can be made available for a fraction of what it would cost developing them internally or procuring them in the open market.
- ✓ Benefits from economies of scale.
- ✓ the goods and services may not be available off-the-shelf.

3. Economy

DIGIT has made an estimation of the costs of the two main control phases : ex-ante and supervisory measures. Benefits of those controls have also been

¹⁹ these amounts represent the chargeback generated in 2019. Nevertheless part of this can be linked to 2018 activities (late cashing) or 2020 activities (advance payment)

identified. When possible they have been quantified. In some other cases, benefits have been expressed through the corresponding relevant non-quantifiable indicator. The criteria for the calculation and the indicators used to assess the efficiency of controls are shown in the Relevant Control Systems in annex 5.

| | Amount | Cost of Control | In % of value |
|---|------------------------|--------------------|---------------|
| Charge back of services (Internal - collected through co-delegations) | EUR 20 701 477 | | |
| Charge back of services (External - collected through Recovery Orders) | EUR 20 701 477 | | |
| Charge back of services (Internal - collected through Recovery Orders) | EUR 20 249 966 | | |
| Total | EUR 156 571 817 | EUR 559 600 | 0.36% |

An estimated EUR 503 640 were invested in ex ante controls related to the charge back of services to other EU institutions, agencies and bodies and the control related to the charge back of services to the other DGs. Thus, 0.32% of the total charge back value was dedicated to ex ante controls. Regarding supervisory measures such as the regular follow-up of the Master Table, the reconciliation of the ROs with the Master Table and the reconciliations of the co-delegated budget lines with the Master Table an estimated EUR 55 960 were invested in controls ex post related to charge back of services, thus 0.04% of the total charge back value.

In 2019 the total for cost of controls amounted to EUR 559 600 which represents of 0.36% of the amount charged back, as it was in 2018 the amount was EUR 549 800 which then represented 0.39%.

| | 2017 | 2018 | 2019 |
|---|-------------|-------------|-------------|
| Cost of control | EUR 464 750 | EUR 549 800 | EUR 559 600 |
| In proportion to amount charged back | 0.46% | 0.39% | 0.36% |

4. Conclusion on the cost-effectiveness of controls

Based on the most relevant key indicators and control results, DIGIT has assessed the effectiveness, efficiency and economy of the control system and reached a positive conclusion on the cost-effectiveness of controls.

DIGIT has made an estimation of the costs of the three main control processes on Revenues (Chargeback): the establishment of the Commission's rights , the recording, follow-up and accounting of the Commission's rights and the supervisory measures. Benefits of those controls have also been identified. When

possible they have been quantified. In some other cases, benefits have been expressed through the corresponding relevant non-quantifiable indicator.

In 2019 the total cost of controls amounted to EUR 559 600 which represents of 0.36% of the amount charged back. The conclusion of the evaluation of costs and benefits of controls performed for the management of the chargeback and of the indicators used to measure their efficiency, as indicated in Annex 5, is that controls performed in DIGIT during 2019 have been cost-effective as the estimated benefits exceeded the estimated costs and the cost of controls compared to the funds managed are considered reasonable. Furthermore the non-quantifiable (n.q) benefits of the controls are of particular importance :

- ✓ The pooling of resources in order to achieve better services at a lesser cost.
- ✓ Efficiency as know-how, capacities and resources developed can be made available for a fraction of what it would cost developing them internally or procuring them in the open market.
- ✓ Benefits from economies of scale.
- ✓ the goods and services may not be available off-the-shelf.

Also the results of controls show the efficiency of those since they served to comply with the deadlines and mitigate the risks that they address. Thus the conclusion is that the applied control strategy is the best suited to fulfil the intended control objectives efficiently and at a reasonable cost. It should remain unchanged.

Other control objectives: safeguarding of assets and information & IT Security and reliability of reporting

Safeguarding of assets

Regarding the **safeguarding of assets**, DIGIT is the Commission's 'management centre' (*centre de gestion*) for all IT equipment installed in the premises of the Commission in Brussels, Luxembourg, Strasbourg and Dublin (Grange). The general policy is that all PCs, laptops, screens, printers, photocopy machines, scanners, servers, network devices, smartphones and tablets have to be mentioned in the inventory. All steps from ordering to decommissioning of a good are recorded and managed through ABAC Assets modules. ABAC Assets is linked with SAP for accounting purposes (valuation and depreciation). The risks linked to procurement procedures and financial circuits are covered within the previous sections. The operational risks are limited as many inventory actions are automatized.

During its life cycle at the Commission, equipment sometimes needs to be moved. The operation follows the official move procedure under the overall coordination by OIB and OIL - or is launched by a duly justified request from the IRM concerned. Once the move is completed, the related requests are 'closed' in ABAC Assets, which automatically updates the inventory. The number and consequently the costs of IT moves are currently being decreased through two initiatives:

- ✓ First, by the 'Fixed IT' policy which aims at not moving an item with its user when it is not absolutely necessary. Today this policy is applied to all PC displays and, in some DGs, to desktop PCs and docking stations.
- ✓ Then, through the implementation of 'digital workplace strategy', all IT

end users will gradually be equipped with 'docked laptops' instead of a combination of desktop PCs and laptops.

DIGIT's assets amount to EUR 32 758 995.

As mentioned in the Relevant control system (see annex 5), controls aim at safeguarding the assets DIGIT purchases and manages on behalf of all the DGs and services of the Commission, such as:

- ✓ Physical check of all assets and non-assets;
- ✓ 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.);
- ✓ (In)tangible assets and inventories follow formal procedures for disposal of assets.

DIGIT has made an estimation of the costs of these controls. Benefits of those controls have also been identified. When possible they have been quantified. In some other cases, benefits have been expressed through the corresponding relevant non-quantifiable indicator. The criteria for the calculation and the indicators used to assess the efficiency of controls are shown in the Relevant Control Systems in annex 5.

In 2019 the total for cost of controls amounted to EUR 842 380 which represents of 2.6% of the assets controlled.

As mentioned in the Relevant control system (see annex 5), a number of controls are in place to ensure the safeguarding of information and IT Security. In order to avoid sensitive information being "lost" (abused, made public) or its integrity breached (data altered), DIGIT makes sure that internal rules on data protection in line with Commission's rule, and internal rules on treatment of sensitive information are being met. Additionally, physical and IT access rights to the financial systems are closely monitored.

2.1.2 Audit observations and recommendations

This section sets out the observations, opinions and conclusions reported by auditors – including the limited conclusion of the Internal Auditor on the state of internal control. Summaries of the management measures taken in response to the audit recommendations are also included, together with an assessment of the likely material impact of the findings on the achievement of the internal control objectives, and therefore on management's assurance.

IAS audits

As of end January 2020, there were 40 recommendations issued for DIGIT, distributed over 11 audits, out of which:

- 16 have been closed by IAS of which 9 in 2019 (as detailed in annex 11);
- 11 are considered implemented by DIGIT in 2019 and have been sent to IAS for review;
- 13 recommendations remain open; of those, three are considered delayed

and one of these is attributed to HR as Chef de File for implementation. Of the 13 open recommendations, four of them are rated "very important".

Follow-up of IAS recommendations

| AUDITS | N° of issued recs | Recommendations status | | | | |
|--|-------------------|------------------------|-----------------|---------------|----------------------|-------------|
| | | Open | Sent for Review | Closed by IAS | Delayed (< 6 months) | Not due yet |
| Final audit reports issued in 2019 -> recommendations not due yet | | | | | | |
| IAS - 2018 - Audit on IT Project management practices for multi-DGs projects | 6 | 6 | | | | 6 |
| Previous years' recommendations | | | | | | |
| IAS - 2018 - Multi-DGs CEF Telecom Governance | 1 | | 1 | | | |
| IAS - 2018 - Intellectual Property Rights | 2 | 2 | | | | 2 |
| IAS - 2017 - Synergy and efficiency review | 3 | | 3 | | | |
| IAS - 2017- IT programme and project management in the HR family | 3 | | | 3 | | |
| IAS - 2017 - Procurement process in DIGIT | 4 | | 2 | 2 | | |
| IAS - 2017 - Corporate IT governance framework and portfolio management | 2 | | | 2 | | |
| IAS - 2016 - Management of IT security | 5 | 2 | 3 | | | 2 |
| IAS - 2015 - Management of Intra Muros | 3 | 1 ^{HR CDF} | 2 | | 1 ^{HR CDF} | |
| IAS - 2014 - Management of European Commission Authentication Service (ECAS) | 8 | 2 | | 6 | 2 | |
| IAS - 2012 - Charge - back process in the Commission | 3 | | | 3 | | |
| TOTALS | 40 | 13 | 11 | 16 | 3 | 11 |

The Limited conclusion of the Internal Auditor on the state of internal control states that the internal control systems in place for the audited processes are effective, except for the observations giving rise to some 'very important' recommendations . These recommendations need to be addressed, in line with the agreed action plans. IAS draws attention to their attendant residual risks.

The "very important" recommendations explicitly mentioned in the Internal Auditor Limited conclusions are detailed below.

Annex 11 provides complementary details on these audits for “important” recommendations and covers audit work carried out in 2019.

IAS – 2015 - Management of Intra Muros

The overall objective of the audit was to assess if the Commission uses the external contractors working intra muros in an effective and efficient way. The audit covered the arrangements both at the corporate level aimed at facilitating the management of intra muros contractors by DGs and the way in which they are managed in practice at the individual DG level.

Two “very important” recommendations were issued by the IAS, of which one addressed to DIGIT and focused on means to control the value for money in ‘Time and means’ contracts. DIGIT duly implemented this second recommendation and notified IAS that it was ready for review in June 2019. At the time of writing, these recommendations are pending IAS review.’ More information in Annex 11.

IAS - 2016 - Management of IT Security (Privileged Access and Vulnerability Management)

The overall objective of the audit was to assess whether the management and control systems in place in the areas of vulnerability management and privileged user access ensure that the ICT systems managed by DIGIT in its datacentres are adequately protected against cyberattacks. Five recommendations were issued in July 2017, out of which two very important related to:

- Assurance on the legitimacy of actions performed in production systems
- Technical inventories of management information for security vulnerabilities

All recommendations and related risks were addressed in an action plan agreed with the IAS in October 2017. Implementation has advanced in line with this action plan and the first very important recommendation has been fully implemented by the end of 2019 as foreseen.

As for the second very important recommendation, implementation is well advanced and expected to be fully delivered by 2020, in line with the target dates. Consequently, most derived risks have been addressed. More on “important” recommendations in Annex 11.

IAS - 2017 - Synergy and efficiency review – Multi-DGs (DIGIT, SG, HR, BUDG, COMM, OIB, JRC, SCIC)

The objective of this audit was to assess whether the Commission has put in place an appropriate framework and methodology, processes and controls to ensure that the objectives of the SER Communication are met. The final audit report includes three recommendations. DIGIT provided inputs for the action plan addressing the recommendations/risks, mostly as a contributor under HR lead, and as leader for the IT domain for parts of other recommendations. In fact, DIGIT collaborated to reaching the objectives of this forward looking project since the SER communication was issued.

The second and third recommendations (very important) are of corporate nature: “Embedding the SER culture Commission-wide” and “Improving monitoring arrangements and reliability of savings estimates”. Both are composed of several sub- actions; DIGIT took the lead as IT domain leader for the following sub-

actions of the second recommendation:.

2.1 contributing to the HR communication campaign to explain the SER objectives, the domain leadership culture and potential added-value for the Commission as a whole;

2.3 contributing to the continuous feedback exercise, to foster domain spirit;

2.4 developing appropriate quality assurance mechanisms vis a vis their client DGs (including the publication of service catalogues, agreeing on the minimum service levels, effective monitoring based on SMART KPIs, feedback and provision for corrective/remedial actions).

DIGIT has implemented each of the above sub-points in due time and indicated them as ready for review by IAS in December 2019.

In relation to the third recommendation, DIGIT contributed to the following sub-parts, as leader/co-owner:

3.4 monitoring whether "saved" resources are in fact working on tasks linked to their previous activities.

3.5. monitoring carefully the reliability of its savings estimates and, if not already done so, developing action plans to deliver the remaining/revised targets.

3.6. measuring and reporting information on other quantifiable and qualitative benefits and costs arising from SER.

DIGIT has implemented sub-points 3.4 and 3.6 in due time and indicated them as ready for review by IAS in December 2019. Sub-point 3.5 due 30/03/2020 has at the time of writing also be implemented and indicated on 18/03/2020 as ready for review by IAS.

In conclusion, all the points addressed to DG DIGIT have been implemented. "Important" recommendations are detailed in Annex 11.

IAS - 2018 - Intellectual Property Rights - Multi-DGs (DIGIT, COMM, GROW, OP, JRC)

The objective of this audit was to assess the adequacy of the corporate framework at central level to ensure an efficient and effective management of IPR, in conformity with the applicable rules, as well as the efficiency of IP assets management at local level.

The audit report includes two very important recommendations for the attention of DIGIT, relating to "software and IT solutions" and the "efficiency and effectiveness of IPR management". The other recommendations were addressed to JRC in charge of this file. Accordingly, DIGIT collaborates closely with JRC. As DIGIT actions depend on JRC's, the action plan submitted to IAS takes full consideration of the actions and implementation dates foreseen by JRC. The first actions planned for mid/end 2019 are implemented, thus related risks already impacted.

In conclusion and considering that,

- ✓ No critical recommendations were issued;
- ✓ No “very important” recommendation with DIGIT as Chef de file is delayed;
- ✓ The one remaining “very important” recommendation from the audit on management of IT security mentioned by the Internal auditor in its Limited Conclusion is being implemented and any derived risks have been addressed;
- ✓ From the other two “very important” recommendations mentioned by the Internal auditor in its Limited Conclusion (audits SER and IPR), that for SER has been fully addressed and that for IPR is partially addressed with full implementation expected by the target date (not yet due);
- ✓ The 13 open recommendations issued in previous years have been subject to action plans approved by IAS, with two recommendations close to full implementation (due dates Q1-Q2/2020) and eleven partially implemented (due date Q4/2020);
- ✓ The six most recently issued recommendations (important) have been subject to a relevant action plan approved by IAS;

the risks derived from all open recommendations have been evaluated by management as fully addressed/partially reduced and do not raise any assurance implication.

BUDG audit

In 2019, BUDG performed one audit in DIGIT related to **the validation of local systems**. The objective was to evaluate the local financial management systems including both the administrative processes designed to assure the quality of the data entered into the accounts, and the IT systems which provide information to the central accounts. BUDG issued 4 recommendations rated “important” which DIGIT provided an action plan duly agreed by BUDG. The implementation is on-going and expected to be finalized by mid-2019.

ECA audits

In 2019, the Court of Auditors performed one audit impacting DIGIT.

SPECIAL REPORT No 14 2019 ‘Have your say!’ Commission’s public consultations engage citizens but fall short of outreach activities

The objective of this audit was to assess whether the Commission’s public consultations were effective at reaching out to citizens and stakeholders and making use of their contributions. One of the audit recommendation issued relates to “Data processing and security”. The implementation of this “important” recommendation, under the lead of DIGIT, is on-going and full delivery expected by mid-2020.

Statement of assurance

The Court of Auditors performed its usual statement of assurance (DAS) exercise related to the reliability of the accounts and the legality and regularity of the underlying transactions. Within the DAS 2019 exercise, a sample of specific transactions has been examined. For the moment, no specific issues have been communicated to DIGIT.

As a result of the overall assessment of audit observations, recommendations and underlying risks, and taking into account DIGIT measures to address them, the management of DIGIT believes that the recommendations issued do not raise any assurance implications and are being implemented as part of the on-going continuous efforts in terms of further improvements.

DIGIT does not consider that the observations made by IAS, ECA and BUDG represent a major deficiency of DIGIT's current internal control framework. This is further strengthened by the Limited conclusion of the Internal Auditor on the state of internal control in DIGIT, which he considers effective.

2.1.3 Assessment of the effectiveness of internal control systems

The Commission has adopted an Internal Control Framework based on international good practice, to ensure the achievement of its policy and management objectives. Compliance with the internal control framework is a compulsory requirement. DIGIT uses the organisational structure and the internal control systems suited to achieving its policy and internal control objectives in accordance with the internal control principles and has due regard to the risks associated with the environment in which it operates.

Following the adoption of the Commission's Internal Control Framework (19/4/2017), DIGIT conducted an overall specific assessment which provided a global overview of the state of play of the internal control. Following the methodology, DIGIT defined the basis for its assessment of the internal control system by setting its Internal Control Monitoring Criteria in the 2019 Management Plan. These same criteria were used for assessing the Principles and Components and a set of indicators including baselines and targets, pertinent for the AAR 2019 were identified. The next step consisted of listing all identified internal control deficiencies that affected financial but also non-financial processes. The identified deficiencies were assessed to determine their impact on the effectiveness of the internal control principles and components and finally of the Internal Control System as a whole. At the same time, DIGIT identified the measures already taken to reduce the severity of the identified deficiencies and the impact of those measures on the overall IC system.

To identify internal control strengths and weaknesses, DIGIT used all information sources available:

- The 2018 HR Staff Survey to which DIGIT had a response rate of 63%;
- The weaknesses identified by the IC team itself, such as numerous and late reporting of exceptions/non-compliance events and the impact of new

GDPR on DIGIT's work;

- The extensive review and update of the 2020 Risk register including anti-fraud related risks;
- Exception and non-compliance reporting was analysed (see section 2.1.1);
- The implementation of the anti-fraud strategy was monitored (see section 2.1.1);
- Audit findings and recommendations were analysed (see section 2.1.2).

Following the overall assessment performed, the following can be concluded:

| INTERNAL CONTROL COMPONENT | CONCLUSION |
|--------------------------------------|---|
| CONTROL ENVIRONMENT | Category 1. The component is present and functioning well, only minor improvements needed |
| RISK ASSESSMENT | Category 1. The component is present and functioning well, only minor improvements needed |
| CONTROL ACTIVITIES | Category 2. The component is present and functioning but some improvements are needed |
| INFORMATION AND COMMUNICATION | Category 1. The component is present and functioning well, only minor improvements needed |
| MONITORING ACTIVITIES | Category 1. The component is present and functioning well, only minor improvements needed |

The internal control annual assessment resulted in a positive result for all components. Components I, II, IV and V are considered present, functioning well and only minor improvements are necessary. All the necessary improvements have been identified for each principle have been included in a yearly action plan which will be duly implemented. Regarding Component III the conclusion is that it is partially present and functioning but some improvements are needed. This is specifically the case for Internal Control Principle 11 which is partially present and needs improvements.

The improvements necessary for Internal Control Principle 11 are mainly influenced by the number of very important open audit recommendations issued by the IAS which are pending implementation and the rapidly evolving area of IT security which forces DIGIT to continuously adapt to new circumstances.

Regarding the open audit recommendations, it should be noted that improvements have already been made compared to 2018 with a decrease of delayed open recommendations and that action plans for most recommendations have been approved by IAS and that they are in the process of being implemented (more details in section 2.1.2.).

Furthermore the following other initiatives and measures are in place or are in the process of being implemented:

- ❖ The provision of better IT Security Services supported by the provision of IT Security operations emphasise prevention and focus on the development and deployment of IT security processes while improving the baseline IT Security of corporate infrastructure. The achievements of the targets set in 2019 can be considered as fully satisfactory, according to the evidence described in part 1 of this AAR;
- ❖ In the wake of the Commission IT Security Strategy adopted in 2016, and in light of emerging new challenges related to IT Security worldwide, DIGIT has updated the Strategy and proposed a new rolling plan covering the period up to 2020. The updated IT Security Strategy – adopted by the ITCB in early 2019 – better defines DIGIT’s role in delivering a number of measures to prevent and fight cyber-security related risks;
- ❖ With over 50 presentations on cybersecurity delivered during the year, and several tailored trainings and briefings targeting a diversified audience, DIGIT successfully achieved the original plan on cyber-awareness among the Commission staff. A 24/7 security operation capability (started as a pilot in December 2019) has already been addressing IT security incidents occurring during critical periods (e.g. during Christmas holidays), although at present maintaining the required staffing level for ensuring the service remains a critical challenge. A well-established and properly functioning IT security governance framework also supports better IT security decision making. For this reason, in 2019 DIGIT developed and documented an IT Security Risk Management Methodology (ITSRM²) allowing system owner to identify, evaluate, document and treat IT-security risks.
- ❖ Furthermore, in 2019 DIGIT continued to focus on the actions related to the Commission’s Data Protection Action Plan (C(2018)7432). A particular attention was given to ensuring that DIGIT staff are well-grounded in the principles of personal data protection and to this end DIGIT senior management sponsored an awareness-raising campaign towards all staff. To ensure up-to-date information for data subjects (especially for citizens) the privacy statements for the principle external-facing services were reviewed and updated.

DIGIT has assessed its internal control system during the reporting year and has concluded that it is effective and that the components and principles are present and functioning well overall, but some improvements are needed as minor deficiencies were identified related to Internal control principle 11. This could in theory have an impact on the assurance, nevertheless considering the remedial measures already implemented and those envisaged (see above), it can be concluded that no reservation should be issued in the AAR.

2.1.4 Conclusions on the assurance

This section reviews the assessment of the elements already reported above (in Sections 2.1.1, 2.1.2 and 2.1.3), and the sub-conclusions already reached. It draws an overall conclusion to support the declaration of assurance and whether it should be qualified with reservations.

The information provided in the various preceding sections covers all budget delegated to the AOD of DIGIT as well as the assigned revenue (Chargeback of services) and the Assets. The information reported is complete and reliable, as confirmed by the statement of the Director in charge of Risk management and

Internal Control in annex 1.

The intrinsic risk for administrative expenditure managed by DIGIT including procurement is relatively low because of the centralised and direct mode of budget implementation. The risks are effectively mitigated by means of controls put in place (see section 2.1.1.). Furthermore the following elements support our assessment :

- Assurance received from DIGIT'S (cross) sub-delegated Authorising Officers and Assurance received for the credits (cross) sub-delegated to other DGs,
- Positive assurance on administrative expenditure given by the Court of Auditors for several years, and again in the annual report 2018 issued in 2018,
- Conclusions of ex-post control indicate no issues with significant financial impact,
- Positive feedback received from inter-DG group of procurement experts (GAMA) concerning the procurement procedures scrutinised,
- Monitoring, registration and analysis of exception reports and non-compliance events indicate no material issues.

Further assurance is obtained by the DG's annual risk assessment which is integrated in the annual planning exercise. Critical risks are identified and they are the subject of management attention; mitigating actions are systematically defined and implemented.

Results from audits during the reporting year did not include any critical findings. The residual risks from audit recommendations remaining open from previous years are not considered to have a bearing on the declaration of assurance. Furthermore the Limited conclusion issued by the IAS concludes that the internal control systems in place for the audited processes are effective, even if the risks derived from the combined effect of the 'very important' recommendations since they are mitigated by the action plans put in place and the advance in their implementation (see section 2.1.2.).

Management has obtained satisfactory evidence that the internal control system is present and functioning but some improvements are needed. Internal control principle 11 is considered partially effective and needs major improvements. Considering the remedial measures already implemented and those envisaged, it can be concluded that no reservation should be issued in the AAR.

Reasonable assurance is the personal judgment of the AOD based on all information at his/her disposal. This information is structured around different pillars, composed of (1) the DG's assessment of its own activities for the management of its resources; (2) the assessment of the activities carried out by other entities to which the DG has entrusted budget implementation tasks; and (3) the assessment of the results of internal and external audits, including the implementation of audit recommendations.

No reservation is made by the AOD in this AAR.

In view of the control results and all other relevant information available, the AOD's best estimation of the risks relating to the legality and regularity for the

expenditure authorised during the reporting DIGIT calculates, in accordance to central services guidance on the content of the AAR, the Most Likely Error (MLE) for the Commission's administrative expenditure (0.50%) as a conservative estimate in order to allow the consolidation of data when determining the amount at risk at payment at Commission level. This percentage corresponds to an estimated overall amount at risk at closure of EUR 1 635 506.

Taking into account the conclusions of the review of the elements supporting, it is possible to conclude that the internal controls systems implemented by DIGIT provide sufficient assurance to adequately manage the risks relating to the legality and regularity of the underlying transactions. Furthermore, it is also possible to conclude that the internal control systems provide sufficient assurance with regards to the achievement of the other internal control objectives.

Overall Conclusion

In conclusion, management has reasonable assurance that, overall, suitable controls are in place and working as intended; risks are being appropriately monitored and mitigated; and necessary improvements and reinforcements are being implemented. The Acting Director General, in his capacity as Authorising Officer by Delegation has signed the Declaration of Assurance.

2.1.5 Declaration of Assurance

DECLARATION OF ASSURANCE

I, the undersigned,

Acting Director-General of DG Informatics

In my capacity as authorising officer by delegation

Declare that the information contained in this report gives a true and fair view²⁰.

State that I have reasonable assurance that the resources assigned to the activities described in this report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

This reasonable assurance is based on my own judgement and on the information at my disposal, such as the results of the self-assessment, ex-post controls, the work of the Internal Audit Service and the lessons learnt from the reports of the Court of Auditors for years prior to the year of this declaration.

Confirm that I am not aware of anything not reported here which could harm the interests of the institution [.

Brussels., 31 March 2020

(e-signed)

Mario CAMPOLARGO

²⁰ True and fair in this context means a reliable, complete and correct view on the state of affairs in the DG/Executive Agency.

2.2 Other organisational management dimensions

This section covers also the Human Resources Management and the Information management aspects. For an extensive reporting on all components, please refer to Annex 2.

2.2.1 Human resource management

The overall level of staff satisfaction & productivity increased since 2016 (63%) to 68% (Staff Survey 2018) During 2019 there was full collaboration with HR on implementing the Fit@Work Strategy and Action Plan. There have been communications to staff on "Digital Break" and "Work-life balance for parents initiatives. The DIGIT Activity fair on 24.09.2019 was part of the European Week of Sport.

During 2019, 97,1% of Learning & Development 2019 budget was consumed. A wide range of career support and development actions have been implemented, such as :

- Individual coaching packages for in the context of the DIGIT Talent Development Scheme (with focus on female talents).
- Active promotion of the AMC's career guidance services to staff
- Open call for expression of mobility into the Data services in DIGIT

Junior and middle management positions were constantly monitored by the DIGIT BC Team. An internal pool of potential management successors is being built up in the context of the in-house AD male & female talent development, by providing individual coaching, career guidance, training

Staff Survey Development Plan for DIGIT has been drafted and mostly implemented (some actions are still ongoing) :

- Wellbeing: various communications to staff on Fit@Work activities and initiatives
- L&D: Encouraging knowledge sharing of colleagues having participated in and L&D activity via Blog on DIGIT intranet.
- Management: Weekly senior management meeting flash reports published for transparency. Monthly "Coffee with Directors" organised as informal chats for management accessibility and silo breaking.

Finally, the BC Team has continued to actively work towards fulfilling its staffing goals in Luxembourg in the context of the Digital Pole.

2.2.2 Information management aspects

In 2019 DIGIT continued to focus on the actions related to the Commission's Data Protection Action Plan (C(2018)7432). A particular attention was given to ensuring that DIGIT staff are well grounded in the principles of personal data protection and to this end DIGIT senior management sponsored an awareness-raising campaign towards all staff. To ensure up-to-date information for data subjects (especially for citizens) the privacy statements for the principle external-facing services were reviewed and updated. After having completed an inventory

of data processing operations in 2018, in 2019 work on transforming old data protection notifications into “records of processing” as required by the new Regulation continued. In line with the general experience in the DGs, DIGIT too has found that this updating and creation of new records of processing is a slow and resource intensive process, so the work will continue into 2020. Privacy statements were reviewed and information for data subjects updated to reflect the new Regulation. In order to assess the potential impact on data subjects of the future deployment of O365, a major data impact analysis (DPIA) was conducted. DIGIT also continues to review its contracts with IT suppliers and where deemed necessary has commenced re-negotiation of the data protection aspects of these to ensure compliance with Regulation 2018/1725. Following a review of resources allocated to data protection in 2018, and in line with the aforementioned Action Plan, DIGIT proceeded to a significant reinforcement of these resources in 2019.

2.2.3 External communication activities

This section is described in detail in Annex 2 of this Report.