Ref. Ares(2019)2257618 - 29/03/2019

European Commission

2018 DIRECTORATE GENERAL INFORMATICS

ANNUAL ACTIVITY REPORT

DIGIT

Informatics

Table of Contents

THE DG IN BRIEF

DIGIT's Mission

The **Directorate General for Informatics** (**DIGIT**) provides digital services that support other Commission departments and European institutions in their daily work and that help European public administrations work better together.

DIGIT delivers digital services that enable EU policies and support the Commission's internal administration. More concretely, DIGIT provides the EU Commission and other European Institutions with the following high quality and innovative solutions:

- **Workplace solutions**: creating new ways of working and collaborating for staff;
- **Business solutions**: delivering secure digital solutions supporting a digitally transformed, user-focused and data driven administration;
- **Infrastructure solutions**: providing reliable, cost-effective and secure infrastructure and services;

Across these domains, the focus is on **effective solutions**: aligning IT investments with business priorities, facilitating relationships with our strategic partners, balancing risk with business value for the Institution.

Additionally, DIGIT is in charge of supporting the **modernisation of public administrations** by **promoting and facilitating interoperability** so that European public administrations can seamlessly cooperate across boundaries, and include businesses and citizens in the process.

Transforming the Commission through IT

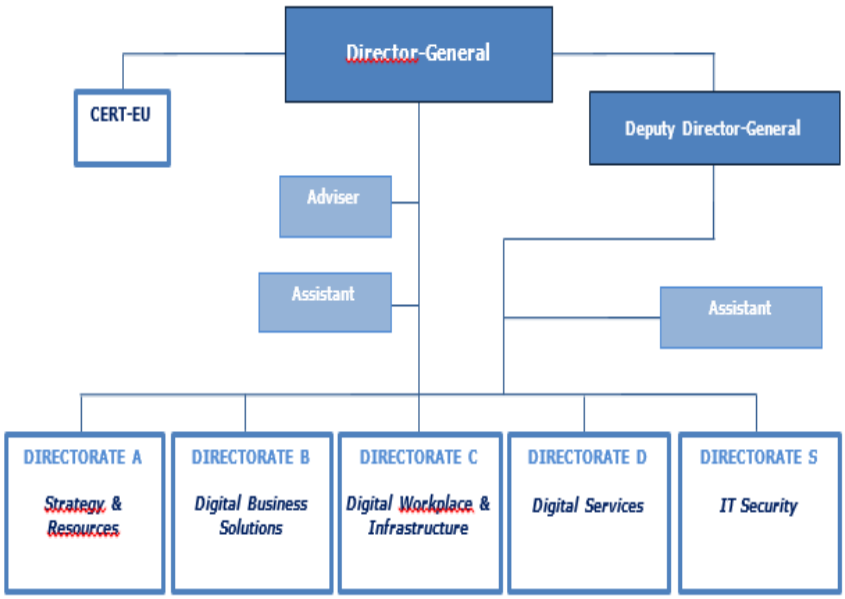
DIGIT's vision

DIGIT has the mandate to lead the digital transformation of the Commission and enable it to deliver EU policy better, more efficiently and more productively, fully seizing the opportunities offered by new technologies.

DIGIT's Partners and Stakeholders

Most of DIGIT's key stakeholders belong to the Commission: end-users for workplace solutions; business owners of information systems for business solutions; Information Resources Managers (IRMs) of the Commission services for infrastructure solutions. However, given its role in the identification of interoperability solutions for public administration, DIGIT also deals on regular basis with Member States, EU and non-EU Public Administrations, businesses and citizens. In this context, the **ISA² Program** represents DIGIT's 'external arm' providing – together with the Connecting Europe Facility (CEF) programme - building blocks and digital services cross-borders and cross-sectors to Member States and other European stakeholders.

Internally, DIGIT is organised in **five Directorates plus CERT-EU**[1], working together closely to achieve its priorities and objectives. As the organisation chart shows, each Directorate focuses on a specific cluster of services (e.g. IT equipment and support, interoperability solutions, hybrid cloud, data centres, customer care, IT and cybersecurity, etc.).



DIGIT operates in a complex and fast-paced environment, and as a consequence, its organisation and way of working has evolved and continues to adapt to keep pace with new challenges in Information Technology.[2]

The Communication on '**Synergies and Efficiencies in the Commission'**[3] was a first milestone in reshaping DIGIT's way of working, enabling DIGIT to steer and lead the ICT domain. Since the introduction of the **Synergies and Efficiencies Review ICT Agenda**[4], DIGIT has been the focal point for identifying upcoming needs and upfront investments in core corporate services, architectural framework and building blocks.

The ICT environment keeps evolving rapidly. The challenge for DIGIT is to find the right balance between technological stability and innovation. This innovation is not only based on using emerging technologies, but also on innovating the processes to build new solutions, using a corporate co-creation approach. This will help the Commission to continue its progress towards a future as a *trustworthy, effective, efficient, transparent and secure* global player.

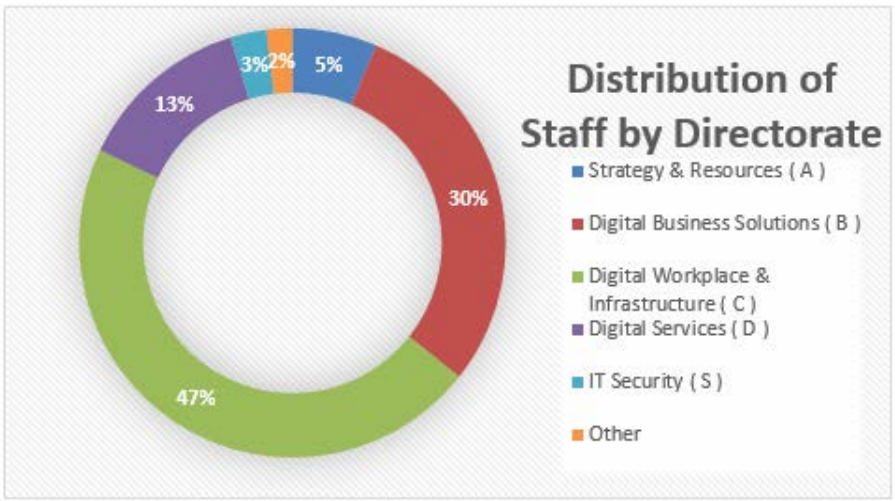
---

[1] CERT-EU (Computer Emergency Response Team) is an inter-institutional body established in 2015. It is administratively attached to DIGIT, but draws up its work plan separately, and reports to an inter-institutional steering board.

[2] DIGIT reorganised in 2017 to respond to emerging efficiency-related challenges.

[3] SEC(2016) 170 final - 04/04/2016

[4] https://myintracomm.ec.europa.eu/hr_admin/synergies/Documents/Synergies%20and%20Efficiencies%20in%20the%20Commission%20-%20New%20Ways%20of%20Working.pdf



In 2018 DIGIT put forward the **European Commission Digital Strategy[5] (ECDS).** The strategy was a response to the Tallinn Digital Summit in September 2017 and the European Council's call - on 19 October 2017 – for '*bringing governments and public sectors into the digital age*'. The strategy addresses major IT challenges beyond 2020, highlights the need to reinforce IT security and points out the importance of data as a catalyst for the decision-making process of the future. It also emphasises that the roadmap to meet these challenges needs to be co-created with all stakeholders. Finally, the strategy enables a business-driven modernisation plan that will provide the Commission with the next generation of digital solutions.

[5] https://ec.europa.eu/info/sites/info/files/strategy/decisionmaking_process/documents/ec_digitalstrategy_en.pdf

EXECUTIVE SUMMARY

The Annual Activity Report is a management report of the Director-General of 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 and for the coordinating, executive and management functions it exercises, as laid down in the Treaties[6].

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

The majority of DIGIT's efforts and ten out of its eleven specific objectives are linked to the general objective shared by the Commission's horizontal services:

'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'.

In 2018, DIGIT continued to deliver on the specific objectives in its Strategic Plan 2016-2020. **Five strategic priorities** guide DIGIT's work towards the modernisation of the Commission, together with the **SER ICT**[7] Agenda that officially enables DIGIT to lead the digital transformation as leader of the ICT domain. In 2018 DIGIT continued to deliver its traditional core activities linked to the provision of IT tools and equipment to Commission staff, reinforced by a far-reaching transformation agenda.

DIGIT contributed to the Juncker Commission priority to establish a **Connected Digital Single Market**[8], by facilitating the modernisation process of public administrations through interoperability solutions under the umbrella of the ISA² Programme and the Connecting Europe Facility. The following sections provide an overview of the major achievements and challenges met in 2018 during the execution of DIGIT's activities as outlined in its 2018 Management Plan:

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

7 DIGIT received the mandate to lead the change process on ICT functioning through the Communication on Synergies and Efficiencies in the Commission – New Ways of Working' on 4 April 2016.

8 https://ec.europa.eu/digital-single-market/

1. Modernisation of public administration:

DIGIT's first priority is to drive the modernisation of public administration in a broad sense. At internal level, this refers to **the modernisation and digitalisation of the Commission's core processes,** exploiting the power of new technologies and business models in compliance with the IT Governance framework. This specific objective covers – to a large extent – the digital transformation agenda of the SER through **three dimensions**. In terms of automation of core corporate processes, DIGIT's expected deliveries advanced well during the year, especially regarding the implementation of the **e-Procurement area** and **SEDIA** (Single Electronic Data Interchange Area, Art. 95 of the Financial Rules). The digital procurement domain progressed well towards the goal of an end-to-end digital solution, capitalising on the architecture and approach successfully applied in the grant management area. The objective is to allow 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. An improved eSubmission service for eProcurement was put in production in May and is hosted in the Secure Hosting Services of the Commission's Data Centre. The "**Funding & Tenders Opportunities**" portal (FTOP) was put in production, and is now part of the SEDIA initiative (Single Electronic Data Interchange Area). The portal is based on a solution initially put in place in the grant management domain. In line with the 'once-only' principle, it now enables suppliers (in addition to grant participants already covered by the SEDIA portal) to enter and send data and documents only once. This produces significant savings both for third parties and for the Commission.

DIGIT continued to contribute to the **innovation of the Commission's legislative lifecycle** and to the roll-out of digital solutions supporting the implementation of policies in the EC and the Member States by expanding **IMI** (Internal Market Information System) and **BRIS** (Business Registers Information System)[9].

"Big Data is high-volume, high-velocity and high-variety information assets that demand information processing enabling enhanced insight, decision making, and process automation"

Big data and data analytics, representing the second strand of DIGIT's commitment towards the digital transformation agenda, went through a significant boost thanks to the endorsement of the **EC Data Strategy Roadmap** and the **DataStrategy@EC Vision** released in April. In the consolidation of this process, DIGIT explored the needs and assets of DGs and services potentially concerned in this domain, in order to establish a community of practice and take on board pre-existing needs and assets. The third dimension of the SER ICT digital transformation, covering architecture components, is now an integral part of the **Reusable Solutions Platform** which has a key role in the EC Digital Strategy. The platform is built around a catalogue containing a corporate architecture, reusable building blocks and services, open-source solutions, standards, best practices, support and consultancy services.

The Catalogue of Reusable Components was extended with 3 more production-ready components: EU Sign, EU Send and API Gateway. More than 20 building blocks already populate the Catalogue

[9] BRIS is a new central platform allowing Member States to implement the 2012 Directive on interconnection of EU business registers.

As part of this initiative, DIGIT has intensified its efforts to roll out well-established reusable solutions (e.g. for notification, search, user interface, electronic signature, etc.) and identify additional ones.

The **modernisation of public Administration** entails DIGIT's involvement also at external level: by exploiting building blocks and interoperability solutions, DIGIT provides a significant contribution to the development of the **Digital Single Market (DSM),** fostering and promoting a modern, efficient and borderless European Public Administration. **ISA²** is the main channel for driving interoperability solutions, together with the **Connecting Europe Facility (CEF) programme**. The work under the ISA² umbrella to offer building blocks and digital services to Member States and other EU stakeholders continued, and the **ISA² Mid Term Conference** in November[10] highlighted the considerable progress achieved. 2018 saw an expansion of contacts and cooperation to third countries[11]: on 29th May, Montenegro joined the ISA² network of 28 EU countries plus Iceland and Norway. In addition, a Memorandum of Understanding was signed with Uruguay, and cooperation with Ukraine was reinforced through an Administrative Arrangement[12] establishing a **knowledge-sharing programme for public administration interoperability solutions.** DIGIT also launched an **Interim Evaluation of the ISA² Programme** in order to assess its performance and to establish whether it was justified to extend the programme after the end of the first mandate in 2020.

2. Create the digital workplace of the future:

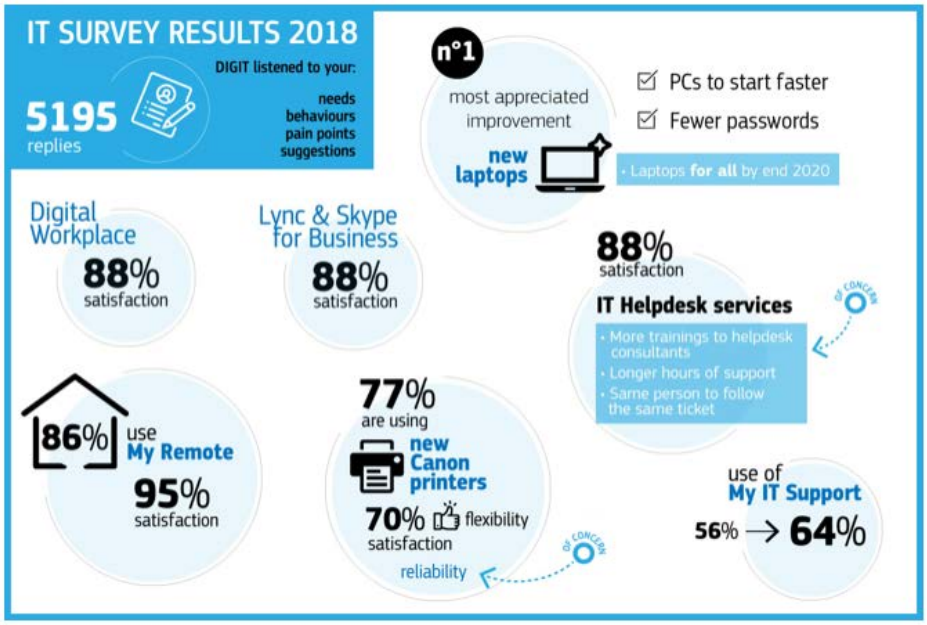
The **Digital Workplace Programme** (DWP) is DIGIT's flagship project to **modernise office automation within the Commission**.

Together with the **standardisation and centralisation of the management of end-user IT** equipment and support services, it underpins the creation of the **digital workplace of the future** (DWP) and covers the actions framed under the SER ICT agenda. The DWP achieved significant progress in 2018, in line with the objectives set in the Management Plan. The most tangible achievement was the **corporate rollout of Windows 10** and **Skype for Business**.

[10] https://ec.europa.eu/isa2/isa2conf18/programme_en

[11] Third countries are not eligible to ISA² funds, but they have access to open source solutions and standards, interoperability frameworks and tools.

[12] https://ec.europa.eu/newsroom/digit/item-detail.cfm?item_id=640975



By year end, **23000 devices were migrated to Windows 10**, with the upgrade including all Commissioners' Cabinets. The introduction of the **Unified Communication and Collaboration** platform (UCC) represents an important change to staff's working practices. Another key delivery in 2018 was the progress on the **transition from desktop to mobile**, which together with the new computer-based telephony will allow staff to '**work anywhere, anytime'**. Close collaboration with DIGIT's IT security Directorate ensured that the new foundation of the Digital Workplace offers a robust environment in terms of cybersecurity and possibilities for mobility and cloud integration.

3. Create the data centre of the future:

DIGIT's third priority encompasses the creation of the data centre of the future by **modernising data centre operations** and by **consolidating data centres**.

In 2018, DIGIT drafted a **revised cloud strategy,** to be submitted to the IT governance bodies early 2019. At the core of this strategy is the vision of a **cloud-first approach** with a **secure hybrid multi-cloud service offering**. In this model, external cloud suppliers complement the service offering of DIGIT's own data centres for those applications where data confidentiality is not a major issue and more agility is required.

DIGIT acted as a 'broker' of cloud services for more than 70 institutions and agencies, significantly boosting inter-institutional cooperation in this domain.

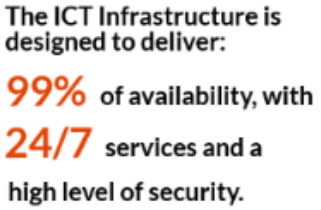
At the same time, DIGIT started **revamping the data centre's delivery model**, leveraging lessons learned from the cloud and applying cloud principles in its own offering. This translates into **increased automation, scalability, self-service and pay-per-use** principles, with a '**private cloud on premise**' pilot deployed in 2018. This 'greenfield' environment will further expand in 2019 and ultimately become the core of

the EC's data centre services. DIGIT's directorates have been working on the implementation of **'DevSecOps'** which - together with the private cloud on premise – will be a game changer on how the Commission develops, secures and operates information systems for the next decades. Concerning the **local data centers** (as part of the Synergies and Efficiencies initiatives), a consolidation programme underpins the new approach for DIGIT's infrastructure service delivery.

Three milestones were met in 2018 in this context: first, the **closure of the local data centres in ESTAT, NEAR and DEVCO**, followed by the **integration of the Publication Office IT infrastructure** in DIGIT, and the **progress made with TAXUD on elaborating a multi-year programme** for the integration of its data centres with the corporate data centres.

4. Better IT Security:

The Commission's IT security Strategy adopted in 2016 gives DIGIT's IT Security Directorate a corporate level mandate to define the action plan for IT security. The SER ICT agenda already identified measures that contribute to the achievement of 3 specific objectives for this domain, namely **strengthened cyber resilience provision of IT security operations** and **better IT security decision making.** The **three pillars of IT security** are covered by a broad set of actions and initiatives that provide better IT security services and increase the effectiveness of the LISO (Local Information System Officer) function. Strengthening cyber resilience across the Commission relies on an efficient baseline IT Security of corporate infrastructures, services and solutions. In the past year, DIGIT's focus was to **ensure that the key IT security processes were implemented in a coherent and consistent way** in all the EC services. Good progress was achieved in the implementation of a **central asset repository for Vulnerability Management**: coverage of vulnerability scans was **extended** to 20% of DIGIT's infrastructure. DIGIT also improved IT infrastructure security – as mentioned in the context of the Digital Work Place above – by focused measures on network segregation, network access control and network encryption. The provision of IT security operations is stable and solid, and in 2018 it kept ensuring security and protection of the IT assets and resources that DIGIT supplies to the whole Commission. This includes detection and monitoring, incident response, and consolidation of IT infrastructures. The Security Monitoring capability has been extended to the new Windows 10 system, while the accessibility of the incident response service remains crucial for reducing the impact of detected security incidents and guaranteeing the eradication of their causes. The next challenge is to streamline and automate the current processes related to infrastructure security and thereby speed up the onboarding of new



clients in this new way of working.

5. Optimisation of DIGIT's delivery:

As a fifth priority, DIGIT is committed to optimising its own delivery **through increasing its customer focus** and **managing better its resources.**

For the customer focus, DIGIT created a customer relationship management function (CRM) in March, which has been building strong ties with DIGIT's customers. The intention is to become a single point of contact for them, always available when needed. The CRM started generating results with a more streamlined gathering and follow up of partners' expectations. This is in line with DIGIT's strategic priority on optimising its external delivery by **seeking alternative ways of simplifying, standardising and consolidating its customer-orientation approach**. Following the 2017 reorganisation, DIGIT can now count on an improved delivery model reshaped to lead the Digital Transformation of the Commission, always keeping an eye on new opportunities for optimising internal efficiency. Additionally, great progress has been made in establishing a Software Factory inside DIGIT to build a harmonized delivery process for Digital Solutions. Tools and methods have been implemented to cover automated testing and code inspections, a key enabler for an effective DevSecOps process. Transparency of costs has also been enhanced, with work towards a consolidated cost model, the scope of which will be reviewed to ensure alignment with the new MFF.

b) Key Performance Indicators (5 KPIs)

Result indicator	Trend	Milestone	Latest known results
KPI-1 The digital transformation composite index Priority: Modernisation of public administration *Source: DIGIT*	☺	In 2017: Value of the index between 10% and 20%. In 2020: Value of the index equal to 50%	2018: 38.24% achieved *Computed based on sub-indicators focusing on business processes and reusable components.*
KPI-2 Overall satisfaction level of the end users with the digital workplace solutions provided by DIGIT Priority: Create the digital workplace of the future *Source: DIGIT satisfaction survey on IT workplace solutions 2017*	☺	Maintain end user satisfaction at least at the level of 80%.	86% of the respondents agree or mostly agree with the statement 'Overall, I am satisfied with the IT workplace solutions and support provided by DIGIT.' *5195 respondents from more than 40 client DGs, Agencies or Services*

Result indicator	Trend	Milestone	Latest known results
KPI-3 Consolidation level of data centres Priority: Create the Data centre of the future *Source: DIGIT*	☺	Target 2019: - 80% of all LDC consolidated into the corporate data centre and Cloud[13]. - Full consolidation of the DIGIT corporate data centre into two main sites (Betzdorf and Windhof)	Year 2018: 25% of consolidation of LDC reached. Clarification to the final target 2019: the multiannual roadmap foresees a commencement of consolidation activities for LDC for 80% of DGs by 2019. In fact, the programme will run beyond 2020. Due to technical and organisational complexity of the consolidation of Local Data Centres process, the original target expected for 2019 has been updated. The final consolidation of this process will only be completed by 2022[14]
KPI-4 Level of IT Security capability Priority: Better IT Security *Source: DIGIT* IT security capability levels are defined based on the scale of the ISO 15504 standard: 5 Optimising process 4 Predictable process 3 Established process 2 Managed process 1 Performed process 0 Incomplete process	☺	Achievement of level 1 in all processes identified as core and level 2 in 50% of IT security processes defined as critical.	Milestone met Core process are defined in the Implementing Rules 2017/8841 of the Commission decision 2017/46. All of them are integrated within the systems lifecycle and performed, attaining at least level 1 on the maturity scale. Some, but not all of them, already reached level 2 or 3. In line with the core concept underlying the provisions of the decision 2017/46, dedicated efforts have been put in place to raise the maturity of the risk management process, relying on the risk management methodology published in 2018.
KPI-5 Availability of a management system allowing flexible allocation of resources to priorities Priority: Optimise DIGIT's delivery *Source: DIGIT*	☺	• Further alignment of DIGIT's Work Programme and budget structure; • Identification of priorities, resources needs and optimisation potentials embedded in the annual planning exercise.	• Budget input structure for 2018 detailed and 2019 Draft Budget (DB) were prepared based on lessons learned from 2017 budgetary exercise; • DIGIT's senior management team (SMT) was invited to provide top-down inputs on priorities before the start of the budgetary exercise; Budgetary request input sheets contained priorities per activity, as well as additional priorities as indicated by DIGIT's SMT
KPI – 6 Estimated residual error rate *Source* : DIGIT AAR	☺	N/A	• Below materiality criteria of 2% (see annex 4)

[13] Note: the 2019 target has been reported to 2022 following the adoption of the new Communication on 'Synergies and Efficiencies Initiative: stock-taking and way forward', on 26/03/2019.

[14] C(2019)2329 Communication to the Commission - Summary of Achievements, Challenges and Way Forward for Support Domains

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

In accordance with the governance statement of the European Commission, (the staff of) 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.

The Commission has adopted a set of internal control principles, based on international good practice, aimed to ensure the achievement of policy and operational objectives. The financial regulation requires that the organisational structure and the internal control systems used for the implementation of the budget are set up in accordance with these standards. DIGIT has assessed its internal control system during the reporting year and has concluded that it is present and functioning but major improvements are needed. Internal control principle 11 is considered partially effective and needs major improvements. This could have an impact on the assurance, nevertheless considering the remedial measures already implemented and those envisaged, it can be concluded that no reservation should be issued in the AAR. 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 aimed to supervise entities to which it has entrusted budget implementation tasks, as well as the observations and recommendations issued by internal auditors and the European Court of Auditors. These elements have been assessed to determine their impact on the management's assurance as regards the achievement of 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 Director General, in her capacity as Authorising Officer by Delegation, has signed the Declaration of Assurance.

d) Information to the Commissioner

In the context of the regular meetings during the year between the DG and the Commissioner on management matters, also the main elements of this report and assurance declaration have been brought to the attention of Commissioner Gabriel, responsible for DIGIT.

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

The following chapters present DIGIT's 2018 main achievements and encountered challenges, according to set priorities and related specific objectives. An exhaustive overview on the work delivered per 2018 Management Plan output can be found in Annex 12 'Performance Tables'.

1.1 Modernisation of public administrations

DIGIT's first priority is the modernisation of public administrations both internally (specific objective 1) and externally (specific objective 2).

Specific objective 1: Drive modernisation and digitalisation of core processes, exploit new technologies and optimise IT investments

Most of the 2018 Management Plan outputs under this objective are linked to the SER ICT digital transformation agenda, structured around three dimensions:

A) The automation of core corporate processes

In terms of **automation of core corporate processes**, DIGIT's expected deliveries advanced well during the past year, especially in regards of the implementation of **SEDIA** (Single Electronic Data Interchange Area, Art. 95 of Financial Rules) and in the e**-Procurement area**. The procurement domain is pursuing its transformation toward an end-to-end digital solution, capitalising on the architecture and approach successfully applied in the grant management area. The objective is to allow 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. Concretely, at the end of June the "**Funding & Tenders Opportunities**" portal (FTOP) was put in production: the FTOP portal is part of the SEDIA initiative (Single Electronic Data Interchange Area). The portal is based on a solution initially put in place in the grant management domain: it is an evolution of the ex-Research Participant Portal. In line with the 'once-only' principle, FTOP now enables also suppliers - in addition to grant participants already covered by the SEDIA portal - to enter/send data and documents only once with significant savings for both third parties and the Commission. An improved eSubmission service for eProcurement was rolled out on 31st May. This service relies on the Secured Hosting Services of the Data Centre, simplifying the tasks of Authorizing Officers while guaranteeing the same level of security.

DIGIT expanded **IMI** (Internal Market Information System) and **BRIS** (Business Registers Information System)[15], IT Systems supporting the implementation of policies in the Commission and the Member States .

Finally and importantly, DIGIT met the targets for increased automation of core corporate processes: in terms of document management and archiving, **ARES 3.0** was successfully deployed with a completely new look and feel. The Commission's legislative lifecycle was enhanced by delivering EdiT, a collaborative tool for drafting legislation. Furthermore, the automation of HR processes proceeded as expected, with the timely rollout of **SYSPER** to other institutions and agencies. Also delivered were ASSMAL2, an improved set of modern tools to manage the EU Joint Sickness Insurance Scheme, and a new Staff Matters Portal to ensure effective support on HR issues. The successful delivery of the afore-mentioned outputs represents another important accomplishment for the systematic review of key processes.

B) Big data and data analytics solutions

This is the second strand of DIGIT's commitment towards the digital transformation agenda. The ability to manage data has become a critical factor to the success of organisations such as the Commission. Good data management enables informed decision making and an overall improvement of the policy-making process. In 2018, DIGIT continued its progress towards the digital transformation in this domain through the endorsement of the **EC Data Strategy Roadmap** and the **DataStrategy@EC Vision** released in April. DIGIT launched an assessment exercise to help DGs and services pinpoint their specific needs and assets in terms of data. The results were used to identify strategic goals and actions for the DataStrategy Action Plan, which was endorsed in November.

C) Architecture components

The third dimension of SER ICT digital transformation, covering architecture components, is now integrated into the **Reusable Solutions Platform** mentioned in the EC Digital Strategy. This platform is being built around a catalogue containing reusable building blocks and services, open-source solutions, a corporate architecture, standards, best practices, support and consultancy services, etc. As part of this initiative, DIGIT has intensified its efforts by continuing to roll out well-established reusable solutions (e.g. for notification, search, user interface, notification, electronic signature, etc.) but also by identifying additional ones (e.g. for authorisation, user centricity, electronic

[15] BRIS is a new central platform allowing Member States to implement the 2012 Directive on interconnection of EU business registers.

workflow, etc.).

Concretely, DIGIT has for instance co-created and successfully launched Compass Corporate with the participation of DGs and Services from the Research, ESIF and Relex families. Compass Corporate is a generic workflow engine platform that facilitates the automation of business processes. It allows end-users to manage in a single place all tasks coming from different domains (e.g. Structural Funds, Grants Management, eProcurement, International Cooperation and Development). Because workflows are usually at the core of digital solutions, Compass Corporate has the potential to become a game-changer for services across the Commission.

In the field of **data, information and knowledge management** work advanced as planned: DIGIT provided a solid contribution to the modernisation of the Commission's core processes related to information management. In line with the principle of **rationalisation of contents and resources**, DIGIT ensured regular support to the web presence of the Commission. Concerning corporate IT governance, DIGIT kept playing its facilitator role, being a key contributor in the work that led to the creation of the Information Technology and Cybersecurity Board (ITCB)[16].

As regards the work that the European Parliament assigned to DIGIT in the framework of the Pilot Projects and Preparatory Actions exercise for 2018, the actions concerned were delivered as scheduled. The **Preparatory Action on Data Analytics solutions** for policy decision making started in September following the adoption of the Financing Decision, and relevant pilots have been identified in order to foster data analytics solutions for evidence-based policymaking. In particular, the analysis involved several EU programmes (LIFE, ERASMUS +, Europeforcitizens, CAP). In the context of the **Preparatory Action on Governance and Quality of Software Code** (aka EU-FOSSA), all the actions scheduled have been contracted in spite of numerous procurement challenges and will be delivered in 2019 as expected. The tremendous efforts engaged in 2018 will lead to the official launch of a €1 million 'bug bounty program' focused on the security of open source software in January 2019. Early results show a positive trend and a remarkable public and press reception.

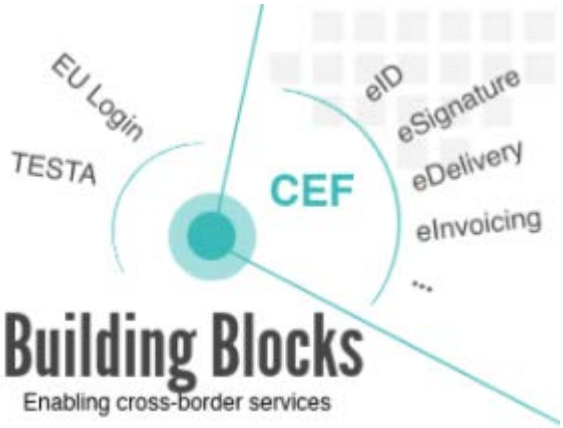
Looking back at the objectives and outputs delivered in 2018 under this first chapter, and keeping in mind the specific priorities that DIGIT defined in its Strategic Plan, the trend for the modernisation and digitalisation of the Commission's core processes is encouraging. At first glance, it shows that the offer of core corporate business processes has increased since 2017. For instance, the rollout of the eProcurement suite together with the implementation of direct grant management for eGrants progressed as expected, producing a positive impact in terms of value for money and optimisation of resources. However, behind the positive outcomes that DIGIT can claim to have reached in the past year, there are evident challenges often inherent to the IT domain itself. The speed and effectiveness of the eProcurement onboarding process amongst the EU Institutions – to give a concrete example – largely depended on whether the Institution concerned was using a certain type of back-office system. In such cases, the need of adapting their own back-office system to the new interoperability standards for public administrations implied that the entire rollout process slowed down or proceeded at a slower pace than expected.

[16] https://ec.europa.eu/info/publications/governance-in-the-commission_en

Specific objective 2: Promote modernisation of European public administrations through the provision of interoperability solutions

Creating a Connected Digital Single Market (DSM) is one of the ten priorities of the Juncker Commission. In the DSM strategy, in particular under the pillar on maximising the growth potential of the digital economy, the public sector and its digital services are of crucial importance. It is within this context that DIGIT – exploiting the potential of the **ISA² programme** – provides solutions to the European public administrations that make them more interoperable and efficient, both within their own departments and towards the businesses and citizens. Following the revision of the European Interoperability Framework (EIF) in 2017, which was included in the Tallinn Ministerial Declaration in October 2017 as a sign of encouragement towards Member States to further apply the EIF, DIGIT continued implementing the new Framework through ISA². The monitoring mechanism of the National Interoperability Framework Observatory (NIFO) was adjusted to guarantee effective monitoring of EIF implementation at both Member States and EU Institutions level.

ISA² reached its midway point in 2018. A **mid-term conference** provided an overview of the major milestones reached during the previous two years of the Programme's lifetime. Strong accent was given to the 28 interoperability solutions already identified, which were showcased in the shape of practical examples from private and public sector. Additionally, in line with the **Better Regulation agenda**, DIGIT launched an **interim evaluation of the ISA² Programme** to assess its performance and to establish whether it was justified to extend it after the end of the first mandate in 2020. The Commission appointed the Centre for European Policy Studies (CEPS) as independent evaluator for this exercise, with the intent to evaluate the programme in its entirety based on 7 different parameters, and identifying areas of potential improvement for which CEPS will be entitled to propose targeted recommendations. Interoperability and digital checks in EU legislation, together with the provision of Connecting European Facility (CEF) Building Blocks, are alternative means for DIGIT to contribute to the Connected Digital Single Market. DIGIT's performance in rolling out the CEF building blocks was again very successful during the past year, with 3 new building blocks launched. Another accomplishment was the endorsement of a new Strategy on **Trans-European Systems Rationalisation** (TES). Following its adoption by Commissioner Gabriel and the IT Board, the implementation of this strategy has been integrated in the setup of the **Reusable Services Platform** (RSP) which is an important part of the European Commission Digital Strategy. The RSP Steering Committee has agreed on the governance model, identified 17 reusable solutions to be included in four waves between 2019 and 2021, and defined work streams with a timeline for each stream. These work streams are the solutions portfolio, governance and funding, cartography and catalogue of services, service framework, quality, and Synergies and Efficiencies (SER) savings.



A detailed overview of ISA[2] actions is available on the Europa site[17]. The box at the end of this section illustrates the EU added value of CEF through a concrete example.

[17] http://ec.europa.eu/isa2

EU ADDED VALUE OF THE CEF BUILDING BLOCKS:

A well-functioning Digital Service Infrastructure (DSI) is pivotal to the success of the Digital Single Market, one of the ten priorities of Juncker's Commission. DSIs are designed to reduce and remove 'digital' barriers preventing EU citizens from using the same goods and services. Digital technologies provide substantial help in facing such challenges, and part of DIGIT's mandate is to foster the creation of cross-border digital infrastructures and services.

Reusable Digital Service Infrastructures – also known as 'building blocks' - provide the necessary technological set-up to facilitate cross-border connections in the framework of the Connecting Europe Facility Programme (CEF). In 2018, DIGIT launched three new building blocks that enriched the existing portfolio of digital services:

- **CEF BDTI – Big Data Test Infrastructure**, which supports public administrations in their quest to turn data into actionable insights;
- **CEF Context Broker,** which centralizes and provides context to data coming from a wide variety of sources;
- **CEF eArchiving,** which enables secure preservation, description and transmission of digital data.

The ultimate purpose of CEF building blocks is to provide fundamental support to the European public services in managing their data, and consequently foster the digitalisation of their public services. In particular, digital building blocks will pave the road for digital transformation of EU Member States, starting at smaller scale in EU cities.

Tangible benefits of building blocks can also be found within the European Institutions: language barriers in the EU Council Presidency could be overcome through **eTranslation**. The twice-yearly rotation of the Council Presidency brings with it considerable linguistic challenges as all official documents and press articles must be translated into 24 EU languages. CEF Translation, using Neural Machine Translation technology, helped to address this problem: **EU Council Presidency Translator** is a machine translation tool. It has increased translation productivity by up to 40%, reducing the workload of translator officials and enabling an international public to self-translate a wider number of documents.

CEF BUILDING BLOCKS AT A GLANCE:

- ***108 known cases of reuse***
- ***42 more cases identified in 2018***
- ***66 out of 108 cases were identified in the EU institutions***

1.2 Create the digital workplace of the future

DIGIT's second priority is to create the digital workplace of the future by providing a modern office automation environment to its users (specific objective 3) and by standardising and centralising the management of end-user IT equipment and support services (specific objective 4). Both these objectives cover actions of the SER ICT agenda.

Specific objective 3: Provision of a modern office automation environment

SECEM 2 and Windows 10 will bring more security to corporate emails and will guarantee easier remote access on your corporate laptop

The Digital Workplace of the Future (DWP) was launched end 2016 in the context of SER ICT. The programme is structured around six strands: devices, office automation, email & calendaring, unified communication, collaboration, and identity & access management. Despite some minor technical issues which caused slight roll-out delays, the DWP progressed well in 2018 in line with Management Plan targets:

More than 65% of EC staff is now equipped with a powerful laptop instead of an old, traditional desktop.

- **Transition from desktop to laptop*:*** there were some initial delays due to patching measures to reduce Spectre and Meltdown vulnerabilities. Secondly, the transition advanced at slower pace in the first quarter of the year due to the fact that new laptops are Windows 10 only, and therefore users who had not migrated to Windows 10 could not change laptop. DIGIT put in place adequate countermeasures which accelerated the transition and its successful completion within the target defined in the Management Plan. The transition will be fully completed by 2020.
- **Improvement of mobile services: as** Microsoft ceased support for the initially agreed design of mobile services, a significant change in the technical architecture had to be made.
- **Office automation:** the successful rollout of Windows 10 is one of the most concrete achievements in the Digital Workplace. DIGIT promptly addressed the issues raised during the first steps of the migration and completed the process by the end of 2018. At present, 23.000 devices have been migrated to Windows 10, including all Cabinets. In some DGs, some delays occurred due to end-of-year priorities.
- **Email and Calendaring:** the migration on the new email platform (Exchange 2016) started on schedule. A number of serious hardware defects delayed the project and were fixed with the help of suppliers. The migration was resumed without affecting the overall objective.
- **Unified Communication (UCC):** phasing-out of legacy telephony reached the target of 21% of fixed telephone sets removed by the end of the year. The technical complexity of the old telephony integration, together with some reluctance of end-users in accepting this change, were two major risks for this activity. DIGIT managed to avoid jeopardising the phase-out process by dedicating more efforts to communicating and demonstrating what was changing

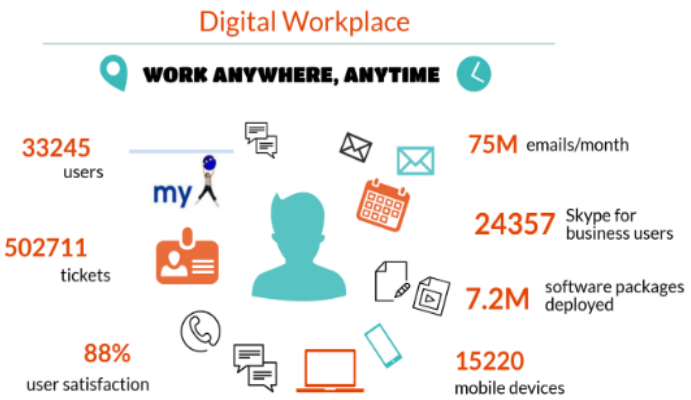
with the introduction of UCC telephony services. By year end, the UCC rollout was completed in 75% of DGs.

- **Integration and Identity & Access Management:** 3 pilots on cloud integration and on premise services within the hybrid platform were successfully completed. The actual integration process was slowed down due to resource constraints.

Specific objective 4: Standardised and centralised management of end-user IT equipment and support services

In 2018, DIGIT continued improving and consolidating the centralised management of end-users equipment and support services, an activity covered by the SER ICT Agenda. The focus remained on standardisation and centralisation of ICT equipment within the Commission. As part of the simplification of the IT equipment management model, DIGIT could offer new services to DGs in terms of centralised processes. This could replace the decentralised processes previously relying on the role of IRMs. The architecture for identifying new processes for the optimisation of IT logistics was defined by the end of the year, as scheduled.

The results of the IT Annual Survey show that the satisfaction level of end-users with the IT Helpdesk support, a Key Performance Indicator for the quality of "IT services that fit users' needs", remained stable and above the predefined target of 80% of overall satisfaction. This proved that following the introduction of "My IT Support" (which complements the existing EC Helpdesk system), the Commission's end-users are satisfied with the support services currently offered when a technical incident occurs. In order to further increase the quality of IT support, and consequently increase the users' satisfaction, DIGIT continued exploring new paradigms and channels for user support through information sessions and specific consultancies.



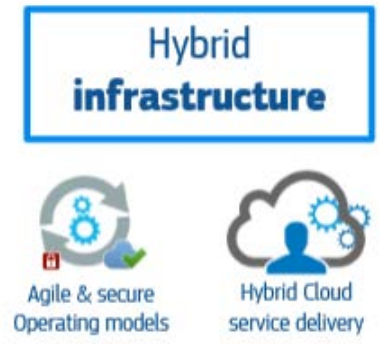
1.3 Create the data centre of the future

DIGIT's third priority is the creation of the data centre of the future by modernising data centre operations (specific objective 5) and by consolidating data centres (specific objective 6).

Specific objective 5: Modernised data centre operations towards a hybrid cloud

The outputs related to the modernisation of data centre operations were delivered as planned. DIGIT continued the successful implementation of a Cloud Broker Service in order to provide Cloud resources and manage cloud contracts for the whole Commission, and the streamlined service could be published on the Service Catalogue. One of the major changes in 2018 was the move towards a **Cloud Strategy** that will replace the European Commission Cloud Governance. The idea behind the Cloud Strategy is to face the need of transforming the way we deliver IT solutions through the Cloud.

Amongst new DevSecOps services released in 2018, there is the first version of the DEVELOPER WORKSTATION, already published in the Service Catalogue



33 DGs and 12 EU Institutions are already exploiting the Cloud Broker Service

In particular, the **hybrid approach** is the main pillar of the future Strategy, as it relies both on Multiple Public Clouds and on EC Managed on-premise Private Cloud. The hybrid infrastructure is built with agile and secure operating models, and leads to a hybrid service delivery.

The **Private Cloud on EC premises** would be managed with a high level of control, and would guarantee a set of core-optimized services. At present, the construction of the cloud on premise infrastructure is in progress. Finding staff with the required expertise is the major challenge for a smoother execution of the work. A 'private cloud on premise' pilot was successfully deployed in 2018, resulting in a new environment which will be the core of the data centre of the future.

The **Public Cloud**, scalable and elastic, can still guarantee high level of security despite its 'public' connotation. To this end, new development methodologies have already been explored within DIGIT, with DevOps and DevSecOps being the latest success of this research. DevSecOps, entailing a close and continuous collaboration between developers, security and operations staff, will be a game changer for the Commission.

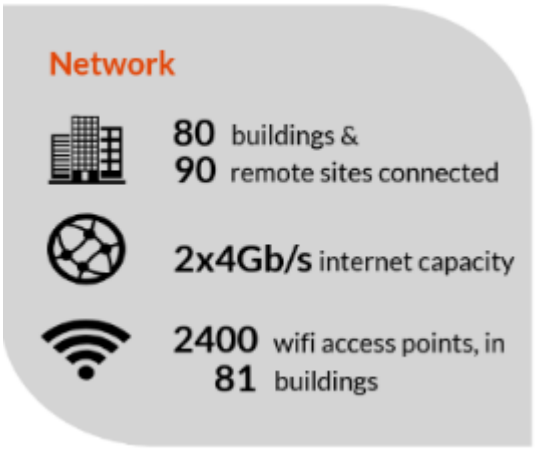
The new Secure Hosting offering is also a growing success, with more and more critical information systems onboarding. Following the joint risk assessment with DG CLIMA, it has been formally proved that such service delivers a structural risk decrease of 3 points based on a risk scale from 1 to 10.

This shows that the secure hosting initiative has delivered on expectations, even those of the most demanding clients.

Specific objective 6: Consolidated data centres

Following the relocation of the JMO data centre towards the new site in Betzdorf, the consolidation of the local data centres (LDCs) proceeded at good speed. Consolidation was fully achieved in DG NEAR, DG ESTAT and DG DEVCO, as targeted in the Management Plan. The ultimate phase of migration activities is ongoing in DG TRADE, DG COMP and DG GROW, while due diligence studies for the consolidation of new local Data Centres were finalised for DG CNECT, DG SANTE, RTD.

- **3 LDC consolidated (DG ESTAT, DG NEAR, DG DEVCO);**
- **Integration in DIGIT of OP IT infrastructure**
- **Launch of multi-year program to integrate DG TAXUD data centre within DIGIT's corporate data centre.**



The new site in Betzdorf has been going through an expansion. DIGIT worked in close collaboration with Luxembourg's central IT services (Centre des Technologies de l'Information de l'Etat, CTIE) for the procurement process to create the new space in Betzdorf. The expansion process encountered some delays due to the sudden bankruptcy of the selected contractor. A new procurement process had to be launched and completed, and the enlargement of Betzdorf is currently in progress.

1.4 Better IT Security

To effectively and efficiently safeguard its assets (general objective I), the Commission aims to better address the challenges and risks related to IT security. Also, IT security covers an important part in the SER ICT agenda. DIGIT is a key player in this overarching, horizontal domain and defined three specific objectives for 2016-2020.

In order to progress towards the implementation of these objectives, DIGIT.S has closely collaborated with the Directorate for Security (DG HR/DS), CERT-EU, and other relevant European Institutions. This has ensured proper information sharing and coordination of responses to IT security threats and incidents, a well-established practice within DIGIT.

In terms of governance framework of the IT Security domain, in 2018 DIGIT made important steps forward, launching the **revision of the IT Security Strategy**. Following on the IT Security Strategy 2017-2018, the revised Strategy defines a series of actions for four long-term objectives (governance and awareness, IT security processes, monitoring and response, infrastructure security). Addressing the security aspects of Commission's IT systems, the Strategy responds to the latest challenges related to cyber security. DIGIT has a central role in delivering a large number of actions proposed in the new IT Strategy, focusing in particular on the reinforcement of the corporate information

assurance service (for instance supporting system owners with risk assessments) and on corporate security assurance (for example, by performing penetration tests and vulnerability scans).

Specific objective 7: Strengthened cyber resilience

This specific objective is focused on prevention. This implies the development and deployment of IT security processes while improving the IT Security baseline of corporate infrastructures, services and solutions. Steady progress can be reported on both related outputs, which is often the result of close cooperation among various DIGIT units. In terms of IT security processes, work advanced well, as all equipment needed was delivered on time, and good progress was made in the extension of vulnerability scanning services for corporate infrastructure.

On the infrastructure side, the overall target has been fully met: segregation in the Digital Workplace environment and in the data centre (on-premise cloud) were set up.

Specific objective 8: Provision of IT security operations

In order to secure and protect the IT assets and resources provided by DIGIT for the entire Commission, this specific objective covers security monitoring and detection, incident response and IT security infrastructure consolidation both in Luxembourg and Brussels. DIGIT is responsible for the elaboration, maintenance and extension of Security Monitoring (SOC), Information Security Incident Management (CSIRC) and Security Operations Engineering (SOE). As per this first strand of activities, DIGIT ensured the Security Monitoring Capability of all new Windows 10 systems. The launch of the new EnCase solution improved the efficiency of the Security Incident Response: since its deployment, the EnCase tool has allowed the IT security incident handlers (DIGIT CSIRC Team) to acquire evidence and artefacts from infected computers in order to analyse and consequently properly respond to security incidents.

To raise awareness among the Commission's IT professionals, DIGIT has promoted the existence of CSIRC's security, monitoring and response services, which are already part of our Service Catalogue.

CSIRC security, monitoring and response services Team was introduced in 2018 in order to increase the awareness raising amongst Commission's IT professionals

A particular emphasis was given to raising awareness of system owners and other EC stakeholders. According to the latest indicators provided by the CSIRC Team, the current level of system owners' awareness has reached 47%. This value is quite promising, considering the final target of reaching a 90% awareness level between Security Operations by 2020.

Following the IAS recommendation for the improvement of the change management process for DIGIT.S infrastructure, a detailed ITIL Maturity Assessment Report was drafted to address – amongst other issues – an enhanced change management process. In order to improve the baseline monitoring of DIGIT data centre, the security monitoring services are integrated natively in the Cloud on Premises project: this means that security monitoring services is integrated at the design phase. This ensures that such services are extended to all systems that will migrate to this new infrastructure.

Specific objective 9: Better IT security decision making

This specific objective aims at ensuring efficient IT security governance, keeping the Commission's IT security strategy and policy up to date and informing IT security stakeholders such as managers, IT experts and end-users about IT security threats and relevant internal rules.

In 2018, work progressed as planned, and DIGIT regularly informed stakeholders on the current global IT security risks and threats. DIGIT also developed and documented the IT Security Risk Management Methodology (ITSRM^2), that 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.

Besides the consolidation of the IT Security governance role as a means to implement and support important decision making processes in compliance with the corporate IT security strategy, DIGIT actively promoted the 'Cyber Aware' sessions, obtaining a coverage of 75% for all users (35% of VIP/management and 40% of all users informed in face-to-face sessions). This is an important achievement as the general customer satisfaction even exceeds the original 2018 target. The overall status of the 3 outputs linked to this specific objective is fully on track.

As additional support to the implementation of the IT security policy at corporate level, a Central LISO Team was established using the available resources (LISO from DIGIT, PMO and RTD). Information and knowledge sharing ran smoothly thanks to a set of sessions that DIGIT organised for a targeted audience (general staff, Management, LSO, developers, communication specialists, etc.). DIGIT also provided assistance and coaching on a continuous basis, and consistently improved the overall information structure through a sharepoint site, FAQ section, specific action plans and dedicated meetings.

1.5 Optimisation of DIGIT's delivery

To be a trusted partner and a credible change agent in the digital transformation, DIGIT committed, as a fifth priority, to optimise its own delivery through increasing its customer focus (specific objective 10) and managing better its resources (specific objective 11).

Specific objective 10: Increased customer focus

In order to increase its customer focus, DIGIT set up a Customer Orientation Strategy

and Roadmap in 2015 that was redefined and implemented over the following 2 years. The strategy paper identified five priorities to transform DIGIT into a trusted business partner: Strategy & Priorities, Listening & Building Relationship, Service Offering, Process & Organisation and Communication. DIGIT has been focusing on presenting a consistent and coherent face to DIGIT's customers, on optimising the processes to deliver end-to-end services, on defining the DIGIT-wide processes to continuously updating its service offer, and on further improving the communication to customers.

This led to the creation of a central Customer Relationship Management (CRM) function focusing on establishing strong relationships with its customers. In 2018 the CRM team consolidated its role by focusing on the customers' needs. The CRM acts as the bridge between DIGIT and its partner DGs, not only in the delivery of services and technical analysis of their needs, but also coordinating proposals for new internal initiatives. It also represents DIGIT in a number of high priority political files, including the European Social Security Number (DG EMPL) and the European Single Maritime Single Window (DG MOVE).

The above-mentioned action contributes to DIGIT's mission to transform the Commission, and represents a step closer towards the assistance given to DGs in their modernisation plans. The team has also managed the whole process of the Annual IT survey. The survey provides feedback on DIGIT's end user services in the context of the Digital Workplace (DWP) and forms the basis for actions. Together with the Communications team, the CRM team led the "DWP Myths and Realities" lunchtime presentations to address colleagues' concerns about the new ways of working in various DGs. Both actions contributed to improving DIGIT's user focus.

Specific objective 11: Optimised resources management

Building on the initiatives launched over the last years, DIGIT has set incremental steps to ensure it works efficiently, focusing on the right priorities with an optimised allocation of resources. Consolidated planning and monitoring of activities – supported by a streamlined budgetary programming – are the key points of this specific objective.

In 2018, DIGIT pursued its efforts to optimise resources allocation against capacity, supported by a strengthened delivery model and a reinforced governance fostered by the Priority Management Board (PMB) and the HR board (HRB).

Substantive progress has been made in implementing a "software factory" inside DIGIT to optimise delivery of Digital Business Solutions. This factory centralises the management of key skills in so-called competency pools (for project managers, frontend- and backend developers, testers, architects etc.), out of which projects are dynamically staffed. Based on harmonisation of core delivery processes – like code management, development frameworks, test automation etc. – advanced software delivery methods have been developed and established. These include automated inspection and testing of code as well as utilising a set of KPIs to follow up on software quality and overall productivity of the factory. These efforts are also a key enabler for an effective DevSecOps process.

Transparency of costs has also been enhanced with work towards a consolidated cost model. Methodology and analytical data from the consolidated DIGIT cost model are available and now have to be adapted to the new needs of the MFF 2021-2027. The review of financial circuits has been launched and will continue in 2019.

2. ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL

This section explains how DIGIT delivered the achievements described in the previous section were delivered by the DG. It is divided in two subsections.

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

2.1.1 Control results

This section reports and assesses the elements identified by management that support the assurance on the achievement of the internal control objectives. The DG's assurance building and materiality criteria are outlined in the AAR Annex 4. Annex 5 outlines the main risks together with the control processes aimed 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 2018.

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	

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 2018, nine procurement procedures were launched for a total value of EUR 3 012 876 790.

Procedure Legal base	Number of Procedures	Amount (€)	Representing … % of total value
Open Procedure (Art. 104(1) (a) FR)	5	EUR 2 868 359 509	95.20%
Exceptional Negotiated Procedure without publication of a contract notice (Art. 134 RAP)	2	EUR 144 245293	4.79%
Negotiated procedure middle value contract (Annex 1 - 14.2)	2	EUR 271 988	0.01%
Total	**9**	**EUR 3 012 876 790**	

Two negotiated procedures without prior publication of a contract notice (Art. 134 RAP) with a value above Directive threshold ("the procedures") are reported in:

- ✓ 1 procedure is linked to an expenditure ceiling increase for existing contracts for acquisition of information system and web infrastructure solutions development, support, engineering and testing services (with legal basis in Article 134(1)(e) RAP - provision of new services consisting in the repetition of similar services). The ceiling increase was necessitated by the faster than expected consumption of the ongoing framework contracts attributable to DGs other than DG DIGIT. In those circumstances, the ceiling increase became necessary to ensure the provision of the services without disruption until the migration to new framework contracts. The complexity of DIGIT's framework contracts, which in this area are used by several DGs, requires long planning and preparatory cycle; for this reason launching urgent open calls for tenders to solve ceiling difficulties is often not a feasible alternative.
- ✓ 1 procedure aimed at signature of a new contract for continued use of associated high-level services closely linked to a proprietary software used by the Commission and many other EU Institutions (with legal basis in Article 134(1)(b) RAP - technical reasons and protection of exclusive rights). The software vendor – owner of the proprietary software is the sole economic operator possessing the expertise to provide related high-level services that are intrinsically linked to the related software. This procedure ensured operational continuity of the information systems used by the Commission and many EU Institutions through the provision of the necessary support and other associated services.

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. In 2018, out of the

nine procedures launched, seven of them fell under the scope of procedures potentially examined by the GAMA (open procedures and exceptional negotiated procedures). From those seven, four were selected for examination by the GAMA, which issued four positive opinions. In terms of financial volumes, this means that around 73% of the financial volume corresponding to awarded contracts in 2018 has been examined and found compliant with the procurement rules. Finally, during the standstill period (award stage), none of the nine procedures was challenged by the unsuccessful tenderers.

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	329 177 095 €	4646
Payments made	302 147 165 €	7 868
Total	**631 324 261€**	**12 514**

The total amount of 2018 commitment appropriations represents EUR 339 651 415, the execution rate of these appropriations for 2018 is 96.92% which represents EUR 329 177 095, the remaining appropriations will be executed in 2019. The authorised payment appropriations, including the amounts carried over from 2017, represent EUR 458 298 145. Payments made during the financial year amount to EUR 302 147 165 which represents an execution rate of 65.9 %.

During 2018, a total of 7 868 payments were made, amounting to EUR 302 147 165. 98.50 % of these payments were made on time, with an average payment deadline of 12.9 days. 256 payments were suspended for an average suspension period of 46 days. An amount of EUR 11 498,39 was paid as interest due to late payment , representing only 0.0038% 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 361 recovery orders sent out in 2018, only 8 concerned recovery of payments or late interest penalties for an amount of EUR 653 339 (representing 0.22% of the payments made). The other 353 recovery orders concerned chargeback (see page 39).

Following re-engineering of the financial management process in 2016, DIGIT's senior management decided to decentralise the function of AOSD for commitments. In 2018, 100% of the 4 646 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. As foreseen in the

action plan of the 2017 Audit on procurement, a review of the sensitive functions within DIGIT was performed.

During the reporting year, there were 111[18] 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 2018 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, two exception events were recorded. The first concerned a misinterpretation of art. 114a of the Financial Regulation (art. 172 in new Financial Regulation, regarding the renewal extension of framework contracts). The second concerned the frontloading of leasing and maintenance services for early 2019.

A first analysis of the typology of 2018 non-compliance events seems to indicate that the same problems persist from previous years, despite the actions already taken in 2018 such as the review of the procedure.

Indeed:

- 46.8% of non-compliance events relate to the late renewal of software licenses or maintenance of those licenses,
- 21.6% relate to the late renewal of Specific Contracts for External Service Providers
- 9.9% relate to the late renewal of hardware maintenance contracts

The remaining 23.4% concerned a variety of other issues.

Further actions will be taken in 2019, with the objective to raise further awareness and follow-up of the files, a quarterly reporting to the Senior Management will be submitted. Additionally, the use of the software asset management tool in the future will be explored to see if we can use it in order to reduce the number of late renewals of licenses (number one issue above).

In conclusion, the analysis of the available control results, the assessment of the weaknesses identified and their relative impact on legality and regularity has not unveiled any 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%)[19].

[18] 26 of these events originated from other DGs.

[19] It should be noted that out of the 361 recovery orders sent out in 2018, only 8 concerned recovery of payments or late interest penalties for an amount of EUR 653 338.92. The other 353 recovery orders concerned chargeback; therefore we have adjusted the ARC from 0.1% to 0.0%.

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 1 510 735,85.

This is the AOD's best, conservative estimation of the amount of relevant expenditure during the year (EUR 302 147 165,06) 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.

Table - Estimated overall amount at risk at closure

DIGIT	'payments made' (FY; m€)	minus new[a] prefinancing	plus cleared prefinancing	"=Relevant expenditure" (for the FY)	Average Error Rate (weighted AER; %)	estimated overall amount at risk at payment (FY; €)	Average Recoveries and Corrections (adjusted ARC; %)	estimated future corrections [and deductions] (for FY; €)	estimated overall amount at risk at closure[e] (€)
	1			*2*	*3*		*4*		
	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)	based on 7Y-avg historic ARC (as per ABAC DWH BO report on corrective capacity), but to be adjusted to be the best but conservative estimate for the current MFF	= (5) x (8)	= (7) – (9)
	302 147 165 €	**- €**	**- €**	**302 147 165 €**	**0,5%**	**1 510 736 €**	***0.0%***	**0**	**1 510 736 €**

1) Payments made or equivalent, such as after the expenditure is registered in the Commission's accounting system, after the expenditure is accepted or after the pre-financing is cleared. In any case, this means after the preventive (ex-ante) control measures have already been implemented earlier in the cycle.
2) For the purpose of equivalence with the ECA's scope of the EC funds with potential exposure to L&R errors (see the ECA's 2017 AR methodological Annex 1.1 point 15), also 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.
3) Over the past years, the implementation of ex-ante and ex-post controls has not resulted in any 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 no estimated future financial corrections (0.0%). 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.
4) It should be noted that out of the 361 recovery orders sent out in 2018, only 8 concerned recovery of payments or late interest penalties for an amount of EUR 653 338.92. The other 353 recovery orders concerned chargeback (see page 16); therefore we have adjusted the ARC from 0.1% to 0.0%.

Fraud prevention and detection

DIGIT has developed and implemented its own anti-fraud strategy since 2013, elaborated on the basis based on the methodology provided by OLAF. It has been last updated mid-2017 taking into account the 2017 DIGIT reorganisation. 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 2018, 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
- the Director General sent a reminder about confidentiality requirements in September 2018 to the staff of DIGIT
- a reminder was also sent by DIGIT RMIC Director to the Directors of DIGIT and HR directors of all Commission services highlighting best practices on the day-to-day management of Intra-muros consultants
- During the reporting year, OLAF has not initiated any case, which concerns the activities of DIGIT.

DIGIT considers that its fraud prevention and detection strategy is working well; it will however revise its anti-fraud strategy in 2019 to take into account the new Commission anti-fraud strategy to be adopted by mid-2019, and take advantage of the enhanced support offered by OLAF, for example regarding fraud-awareness trainings/actions. More actions might be developed on issues such as conflict of interests, handling of sensitive information, use of insider information, and risk of collusion.

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 ISA^2 program. In 2018 DIGIT granted 12 cross-delegations, on which EUR 10 945 253 were committed during 2018 and EUR 10 522 944 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 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. Information on the cross-sub-delegated credits is provided in the table in annex 11.

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 2018, a total of 7 868 payments were made, amounting to EUR 302 147 165. 98.50 % of these payments were made on time, with an average payment deadline of 12.9 days. This indicator has remained quite stable over the years and the average

payment deadline has even decreased significantly since 2015.

	2015	2016	2017	2018
% Payments made on time	97%	98.5%	98.5%	98.5%
Average payment deadlines	17.1	13.2	13.5	12.9

3. Economy

DIGIT has made an estimation of the costs of the three main control phases: procurement, financial transactions[20] 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 2018 is EUR 3 012 876 790 which represents a major increase as compared to last year this is mainly due to the renewal of 2 Framework contracts which had a value of around 2 billion euros by themselves. It is expected that this value will drop next year as no major Framework contract is expected to be renewed.

	2015	2016	2017	2018
Value procurement	EUR 494 765 319	EUR 770 287 070	EUR 1 214 411 872	EUR 3 012 876 790
Increase of value in %	-	55.7%	57.7%	148.1%[21]
Cost of control (ex ante)	EUR 1 475 100 (0.30% on total value)	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)
Cost per procurment procedure	EUR 134 100	EUR 157 372	EUR 142 665	EUR 155 584

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).

[20] This includes committing and paying of appropriations
[21] 2018 is an exceptional year due to the high value in procurement related to the renewal of 2 major Framework contracts

For procurements, an estimated EUR 1 400 260 was invested in controlling (ex ante) nine procurement procedures for a total value of EUR 3 012 876 790 or 2018. Thus 0.046 % of the total contract value was dedicated to ex ante control and each procurement procedure had an estimated cost of EUR 155 584. Compared to last year, this represents a decrease (0.14% in 2017) of the proportion of the total contract value dedicated to control but as mentioned above 2018 is 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 it's 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 253.57 is the cost per transaction, EUR 3 173 205 is the cost of control which represents 0,5% of the value transactions made. The cost per transaction has decreased with 25 % in comparison to last year (EUR 338,25 in 2017) while the amount of financial transactions has increased with 12.8%.

2018	Amount	Number	Cost of control	In % of total value	Cost per transaction
Commitments made	EUR 329 177 096	4646	EUR 1 654 875	0.50%	EUR 356,19
Payments made	EUR 302 147 165	7868	EUR 1 518 330	0.50%	EUR 111,01
Total	**EUR 631 324 261**	**12514**	**EUR 3 173 205**	**0.50%**	**EUR 253,57**

DIGIT revised its **ex-post control** methodology (as also foreseen in the action plan of the 2017 Audit on procurement) and chose to perform at least once a year a more specific ex-post control exercise 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. The 2018 ex-post control exercises covered:

- ✓ low and very low value procurement procedures (below EUR 60 000) in order to see the evolution since the 2017 IAS audit for a total amount of EUR 92 092;
- ✓ paper invoices registration procedure and their payments for a total amount of EUR 8 417 212.

The total amount verified was EUR 8 509 304 which represents 2.82 % of the total amount paid[22]. The amount controlled last year was EUR 9 770 381 (decrease of 12.78% compared to this year) which represented 3.65% of the total amount paid. The Working Group created to conduct these ex-post exercises concluded that:

- ➢ concerning the 2 low procurement procedures examined; no errors were found; for the 5 very low value procurements examined, no award decision were found. This procedural error can be explained by the lack of well-defined internal procedural safeguards. The new internal guidance, models and checklists for (very) low & middle procurement should be finalised by the end of March 2019.

- ➢ for the 9 paper invoices and related payments, no errors were found. However, a written procedure was missing but it is now nearly finalised.

For the ex-post controls performed, an estimated EUR 16 790 were invested in controlling 9 payments and 7 procurement procedures for a total value of EUR 8 509 304. This reprents 0.20% of the value concerned. The cost per control is EUR 1049.38 which cannot be compared to last year as no specific ex-post control was done by DIGIT's Internal Control, because IAS controlled transactions and procurment procedures in the framework of their Audit on Procurement.

	Amount	Number	Cost of control	In % of value	Cost per control
Ex -Post	EUR 8 509 304	16	EUR 16 790	0.20%	EUR 1049.38
Total	**EUR 8 509 304**	**16**	**EUR 16 790**	**0.20%**	**EUR 1049.38**

4. Conclusion on the cost-effectiveness of controls

Based on the most relevant key indicators and control results, DG 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 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 0.046% of the total value of procurement made in 2018. The costs of ex-ante controls performed by the DG on the verification of financial transactions represent 1,05% of payments made in 2018 or 0.50% on all financial transactions made seeing that DIGIT controls commitments and payments. Cost of controls of ex-post verifications represent 0.006% of payments made in 2018 and 0.20% 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. 98.5 %

[22] EUR 302 147 165,06

of payments made on time, time to pay far below the maximum allowed of 30 days (12.9 days for 2018) 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 3 012 876 790	EUR 1 400 260	0.046%
EX ANTE 2	EUR 631 324 261	EUR 3 173 205	0.50%
EX POST	EUR 8 509 304	EUR 16 790	0.20%
TOTALS	**EUR 3 652 710 355**	**EUR 4 573 465**	**0,13%**

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 2018 have been cost-effective as the estimated benefits 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[23].

In 2018 DIGIT collected a total amount of EUR 139 732 859 of charge back of services.

	Amount[24]
Charge back of services (Internal - collected through co-delegations)	EUR 118 678 580
Charge back of services (External - collected through Recovery Orders)	EUR 18 724 962
Charge back of services (Internal - collected through Recovery Orders)	EUR 2 329 317
Total	**EUR 139 732 859**

Controls are in place (see Relevant Control System in Annex 5) to ensure proper charge back of services provided to other the DGs and Services and EU institutions, agencies and bodies. These are based on:

- Services, costs and performance indicators are defined and described in technical documents (services catalogues, hosting proposals, etc.) and administrative and budgetary provisions are set up in Service Level Agreements (SLAs) approved by the Customer and by DIGIT Information on the IT services and their costs are available on-line on DIGIT web pages as well as on request.

- Specific information on the IT services delivered can be found in specific technical (SLAs, hosting proposals, etc.) and administrative (MoUs) documents.

- In some cases, a detailed report ('*Rapport de gestion*') is provided regularly, summarising the achievements and the use of resources (HR and financial execution).

[23] Art. 21 FR
[24] these amounts represent the chargeback generated in 2018. Nevertheless part of this can be linked to 2017 activities (late cashing) or 2019 activities (advance payment)

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 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[25]	In % of value
Charge back of services (Internal - collected through co-delegations)	EUR 118 678 58		
Charge back of services (External - collected through Recovery Orders)	EUR 18 724 962		
Charge back of services (Internal - collected through Recovery Orders)	EUR 2 329 317		
Total	**EUR 139 732 859**	**EUR 494 820**	**0.35%**

An estimated EUR 494 820 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, 0,35 % 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 54 980 were invested in controls ex post related to charge back of services, thus 0.039 % of the total charge back value.

In 2018 the total for cost of controls amounted to EUR 549 800 which represents of 0.39% of the amount charged back. In 2017 the amount was EUR 464 750 which reprsented 0.46%.

[25] Staff costs

	2017	2018
Cost of control	EUR 464 750	EUR 549 800
In proportion to amount charged back	0,46%	0,39%

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 2018 the total cost of controls amounted to EUR 549 800 which represents of 0.39% 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 2018 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 concerned IRM. 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[26] amount to EUR 40 968 470[27].

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.

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.

Over the past 18 months, there were several IT incidents with impact on the availability

[26] Only applicable for intangible assets
[27] As per Annex 3 Table 4

of essential digital solutions (i.e. email) and on data protection. The root causes point to:

- Technological obsolescence; hardware and software errors
- IT operations in complex and legacy environments
- Communication issues

Though these events were linked to issues of data protection or leakage of sensitive information, they were immediately mitigated and reputational damage was kept to a minimum. The following mitigating actions have been already taken:

- During 2018, DIGIT Senior management addressed data protection on several occasions in order to prepare for the expected entry into force of the revised Regulation on data protection (EU (2018) 1725). DIGIT carried out an internal stocktaking to identify all processing operations handling personal data. These operations were then assessed for compliance with the general principles of the revised legislation once it became available and remedial actions initiated where necessary. In alignment with the recommendations of the Commission's Data protection Officer, priority was given to ensuring compliance of those processing operations involving the general public e.g. outward facing web sites. With the adoption of the Commission's Data Protection Action Plan in November 2018, DIGIT also began an examination of how to strengthen its administrative capacity for dealing with data protection issues and in particular the implementation of the above-mentioned action plan in 2019.
- Furthermore, from a corporate point view DIGIT is in charge of promoting and enabling better IT security for the entire commission (see part 1). This includes avoiding the risk of sabotage, destruction of critical documents, damage to equipment, theft of high-value equipment or sensitive information by external parties / contractors; but also the risk of politically or economically motivated computer crime (hacking) to conduct sabotage or espionage against the Commission's IT systems. Work has already been put in place to increase resilience against cyber-attacks:
  - ✓ The Information Security Governance structure established in 2015 provides a foundation for a prioritised and business driven development of IT security capability; it is being adapted to increase alignment with IT investment and planning decisions through a merger with the IT Board to form the ITSB (IT and security board).
  - ✓ An updated IT security strategy and implementation plan will be presented to the information security governance bodies (DISB, ITCB) for approval. It will then provide the basis for specific actions 2019 Work Programmes and beyond.
  - ✓ IT security remains a priority action area in DIGIT's Strategic and Management Plan to improve the IT security of corporate systems and services. The new IT security rules (framework) under Decision (2017/46) and implementing its Rules (2017/8841) are being complemented with adoption of updated standards and guidelines.
  - ✓ An IT Security Risk Management Methodology has been developed and is now being rolled out with supporting tooling to provide a consistent and appropriate support to risk assessment, planning, mitigation and reporting. An initial assessment of the security posture of core critical systems was completed in 2018, which will be progressively extended to the full set of critical systems. As part of the Digital Strategy starting in 2019, an annual IT Security Risk Report will be produced which will provide a picture of the status and evolution of the Commission's IT Security Risk Profile.
  - ✓ The multiannual cyber-security awareness-raising programme started in 2016 will continue in 2019. The efficiency of cooperation and coordination with other Information Security stakeholders (SG, HR.DS, CERT-EU) under the corporate governance (ISSB, CRMG) is being enhanced.
  - ✓ Closer coordination of all DG level LISOs continued in 2018; in particular the pilot of a centralised LISO service providing a "pole of expertise" embedded in DIGIT S has been launched with 7 participating DGs. The C-LISO structure has so far proved useful for a

number of incidents. The pilot will be reviewed in 2019 and proposals presented to the governance level (ITCB and GDR).

- ✓ In addition, the recommendations issued by the IAS in 2017 as a result of their audit on IT security have been addressed in an action plan the implementation of which will be closely monitored.
- ✓ investments in expertise especially for new areas such as cloud and data analytics remain a priority. The on-going migration to Windows 10 and to the consolidation of local data centres is hardening the IT infrastructure.
- ✓ New threat-hunting services have been launched to detect forms of attack that would go undetected by conventional rules based monitoring techniques. The Commission's capability to detect, prevent and respond to incidents in information systems is an emerging challenge. The capacity of the security assessment services has increased substantially in 2018 and will be further developed and industrialised in 2019 to meet high levels of demand for information systems testing.
- ✓ Following a decision of the CMB in September 2018, an operational capability will be launched in 2019 to provide an on-call response to cyber incidents outside standard working hours.

Even though events have had an effect on the reputation of the Commission, management has concluded that there is no material impact on the assurance. Because of the number of mitigating measures already put in place (see above), management is not qualifying the declaration of assurance with a reservation. We can thus conclude that the control objective as regards safeguarding of assets and safeguarding of information and IT Security has been achieved.

2.1.2 Audit observations and recommendations

This section reports and assesses the observations, opinions and conclusions reported by the auditors in their reports as well as the limited conclusion of the Internal Auditor on the state of internal control, which could have a material impact on the achievement of the internal control objectives, and therefore on assurance, together with any management measures taken in response to the audit recommendations.

As of end January 2019, there were 55 recommendations issued for DIGIT, distributed over 13 audits, out of which:

- ✓ 29 have been closed by IAS;
- ✓ 6 are considered implemented by DIGIT in 2018 and have been sent to IAS for review;
- ✓ 20 recommendations remain open (distributed evenly between “very important” and “important”); of those, six were issued early 2019 and are not due yet; of the 14 remaining open only three are considered delayed and one of these is attributed to HR as Chef de File for implementation.

Therefore, there has been a decrease of 70% in the number of delayed recommendations in comparison with 2017. Besides, at the time of reporting, no “very important” recommendation with DIGIT as Chef de file, is delayed for more than 6 months, which is also an improvement.

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 2018 -> recommendations not due yet						
IAS - 2017 - Synergy and efficiency review	**3**	3				3
IAS - 2018 - Multi-DGs CEF Telecom Governance	**1**	1				1
IAS - 2018 - Intellectual Property Rights	**2**	2				2
Previous years' recommendations						
IAS – 2017- IT programme and project management in the HR family	**3**	3				
IAS - 2017 - Procurement process in DIGIT	**4**	2	1	1		2
IAS - 2017 - Corporate IT governance framework and portfolio management	**2**	1	1			
IAS - 2016 – Management of IT security	**5**	5				5
IAS - 2016 - Management of Intra Muros	**3**	1 HR CDF	2		1 HR CDF	
IAS - 2015 - Information Security Governance in the Commission	**4**			4		
IAS - 2014 - Management and Supervision of Contracts for the Outsourced IT Services (IT contract management)	**6**			6		
IAS - 2014 - Management of European Commission Authentication Service (ECAS)	**8**	2		6	2	
IAC - 2013 - External Staff management	**11**			11		
IAS - 2012 - Charge-back process in the Commission	**3**		2	1		
TOTALS	**55**	**20**	**6**	**29**	**3**	**13**

Follow-up of IAS recommendations

- ***During 2018, the following three audits were performed:***

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.

The first, rated "important", relates to "Implementing the SER in practice". It is composed of seven sub-observations, DIGIT is taking the lead only one (building blocks project). This project started in 2018 already and DIGIT drives 6 working groups covering specific topics.

The second and third, rated "very important" are of corporate nature: "Embedding the SER culture Commission-wide" and "Improving monitoring arrangements and reliability of savings estimates". Each of those are also composed of several sub-actions; DIGIT will take the lead as IT domain leader for few of those sub-actions only, most of them being under the lead of HR.

DIGIT provided inputs for the action plan addressing the recommendations/risks, mostly as a contributor under HR lead, or for a few points as a leader for the IT domain. In fact, DIGIT collaborated to reaching the objectives of this forward looking project since the SER communication was issued. Some parts falling under its remit are already advanced (local date centre consolidation, e-procurement, building blocks), reducing the risks accordingly.

IAS - 2018 - CEF Telecom Governance – Multi-DGs (DIGIT, DGT, EMPL, GROW, SANTE, JUST)

The objective of this audit was to assess the adequacy of the design and the effectiveness of the Commission's CEF Telecom governance arrangements, i.e. the structures and processes put in place by the Commission to steer, manage and monitor its activities in order to achieve the CEF Telecom policy objectives. The final audit report includes only one important recommendation addressed to DIGIT. It relates to the proper management of Memorandum of Understanding when DIGIT is the solution provider. An action plan relating to this recommendation has been prepared and is pending the approval of IAS. The implementation date proposed is 30/06/2019, thus it is expected that related risks will be promptly addressed.

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 final 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 will collaborate 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 steps of implementation being planned for mid/end 2019, related risks are thus expected to decrease accordingly.

- ***In 2018, IAS also finalised four follow-up audits:***

2nd follow-up audit on the IAC - 2013 External Staff Management

The remaining five important recommendations have been closed by IAS in March 2018.

2nd follow up audit on IAS - 2014 - Management and Supervision of Contracts for the Outsourced IT Services (IT contract management)

The last important recommendation on the Quality management of time and means services was sent for review end 2017 and closed by IAS in October 2018.

2nd follow up audit on IAS – 2015 - Information Security Governance in the Commission

The last very important open recommendation related to the Integration of Information Security Risk Treatment was considered fully implemented by IAS and thus closed in November 2018.

The implementation of these seven last recommendations, enabled the closure of the related audits.

1st follow-up audit on IAS - 2017 - Audit on Procurement process in DIGIT

The important recommendation relating to ex post control was considered fully implemented by IAS and thus closed in December 2018 (see below for the state of play of the other recommendations).

These four audits enabled the closure of eight recommendations, of which one "very important".

- ***Follow-up of previous years recommendations***

Regarding the implementation of recommendations issued in previous years by the IAS, DIGIT completed the implementation of a number of these:

IAS - 2012 - Charge-back process in the Commission (multi-DGS)

The two remaining important recommendations concerning the Charge-Back Process in DG DIGIT have been sent for review. They relate to the identification of IT services to be charged-back and Communication on costs. The 3rd follow-up conducted by IAS on this audit is on-going.

IAS – 2014 - Management of European Commission Authentication Service – ECAS

The implementation of the two last important recommendations continued in 2018 and is still on-going. They relate to further enhancing the level of the service offered, and improving the security of ECAS. Finalisation of both is expected by end 2019 and beginning 2020.

IAS – 2015 - Management of Intra Muros

Two “very important” recommendations were made by IAS.

Number 1 is in 2 parts; a) at corporate level (led by HR, DIGIT contributor) it requires the definition of a corporate framework for using intra-muros contractors. This aspect remains open and is delayed. Part b of the recommendation was rated important and addressed to DIGIT. It requested analysis of the consequences of using intra-muros and an outline of a future strategy.

The second recommendation, addressed to DIGIT and rated very important, is focused on means to control the value for money in ‘Time and means’ contracts. Both the recommendations addressed to DIGIT have been implemented and IAS has been notified that they are ready for review. The first follow-up audit is on-going.

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:

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

The other three recommendations (important) relate to improving the usability of security logs and updating the IT security Framework derived from the Commission Decision C(2017)46 on the security of communication and information systems in the European Commission. 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 three recommendations (one of which very important) should be fully implemented by the end of 2019 as foreseen. As for the remaining two, implementation has started and they should be fully delivered by 2020. Consequently any derived risks have been addressed

IAS - 2017 - Programme and project management in the HR family (HR, PMO, EPSO, DIGIT)

The objective of the audit was to assess the adequacy of the design and the effectiveness and the efficiency of the governance, management and control systems put in place by the HR family (DG HR, PMO and EPSO) and DG DIGIT to manage IT related or enabled programmes and projects. Three recommendations were issued (two very important and one important). HR as Chef de File in this audit coordinated the preparation of the action plan, which was approved by IAS in February 2018. DIGIT is chef de file only on the second very important recommendation – IT project management. The implementation of this recommendation is quite advanced and should be finalized by the end of Q1/2019, in line with the implementation date foreseen, thus reducing promptly the related risks.

IAS - 2017 - Procurement process in DIGIT

The objective of the audit was to assess the adequacy of the design and the effective implementation of DIGIT's internal control systems for the management of the procurement process and the effectiveness and efficiency of the related financial circuits. IAS issued four important recommendations. One recommendation on "ex-post controls" is closed. The recommendation on "sensitive functions and follow-up of the ABAC access rights review" is considered by DIGIT as implemented and was sent for review. Two recommendations related to "ex-ante controls" and "(very) low value procurements process" are under implementation (due dates in the next months). DIGIT expects to meet the due dates for both recommendations and send them for review to IAS, with thus a likely closure of the audit itself before the end of the year.

IAS - 2017 - Corporate IT governance framework and portfolio management (SG, DIGIT)

The overall objective of the audit was to evaluate the current corporate IT governance arrangements in the Commission. The final report for this audit was received end January 2018 and two very important recommendations were issued:

The first recommendation relates to Corporate IT governance: the role of the IT board should be reinforced and clarified, a mid- to long-term Commission-wide IT strategy defined, and the guidance and support to DGs strengthened (set-up/functioning of local IT governance).

The second recommendation relates to the oversight on corporate IT portfolio; it recommends taking a risk-based approach and extending the IT Board oversight to significant investments needed to run systems/services in DGs. It also requests for significant IT projects/systems/services, the improvement of information presented to the IT Board (covering full life cycle) and the development of a process to assess and monitor their business value (benefits, risks, costs). Finally, the decision making process regarding the allocation of the IT Global Envelope should be streamlined (in respect of the budgetary procedure) and a more equitable model of cost sharing for re-using IT building blocks ensured.

The first recommendation is considered implemented by SG/DIGIT and has been sent for review to IAS in January 2019. The second recommendation is under implementation and scheduled to be complete in early 2019.

Limited conclusion Internal Auditor on the state of internal control

IAS concludes that the internal control systems in place for the audited processes are effective, except for the observations giving rise to the 'very important' recommendations (see above). These recommendations still need to be addressed, in line with the agreed action plans or by the submission and implementation of an agreed action plan. IAS draws attention to the risks, that DIGIT is exposed to, due to the combined effect of the two 'very important' recommendations from the audit on management of IT security in DG DIGIT.

In conclusion and considering that,

- ✓ No critical recommendations were issued;
- ✓ The 14 recommendations issued in previous years have been aligned to action plans approved by IAS, with seven recommendations close to full implementation (due dates Q1-Q2/2019) and four partially implemented (due date Q4/2019);
- ✓ The two “very important” recommendations from the audit on management of IT security mentioned by the Internal auditor in its Limited Conclusion are being implemented and any derived risks have been addressed.
- ✓ For the six most recently issued recommendations (four very important, two important), relevant action plans have been submitted to IAS.
- ✓ Some of the recommendations have an important corporate dimension, which implies that DIGIT is a contributor to the implementation but does not bear the risk on its own;

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

ECA audits

In 2018, the Court of Auditors did not perform any specific audits in DIGIT other than the DAS exercise. Within the DAS 2018 exercise, a sample of specific contracts and procedures has been and is still being verified by the CoA. For the moment, no specific issues have arisen.

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 represent a major deficiency in DIGIT’s current internal control framework. This is furthermore 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 the internal control systems

The Commission has adopted an Internal Control Framework based on international good practice, aimed to ensure the achievement of policy and operational objectives. In addition, as regards financial management, compliance with the internal control framework is a compulsory requirement.

DIGIT has put in place the organisational structure and the internal control systems suited to the achievement of the policy and control objectives, in accordance with the standards and having due regard to the risks associated with the environment in which it operates. During 2017, the transition towards the new IC Principles was prepared with the Director in charge of Internal Control and Risk Management and in 2018 it was fully implemented. The revision of all procedures has already taken place as well as the complete revision of the DIGIT Intranet site on Internal Control and the addition of a SharePoint on IC.

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 2018 Management Plan (and updated them in the MP 2019). These same criteria were used for assessing the Principles and Components and a set of indicators including baselines and targets, pertinent for the AAR 2018 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 was launched and DIGIT had a response rate of 63%.
- Several weaknesses were identified by the IC team itself, such as numerous and late reporting of exceptions/non-compliance events, the untimely availability of Framework Contracts (late procurement procedures), the impact of new GDPR on DIGIT's work.
- The extensive review and update of the 2019 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 3. The component is partially present and functioning, major 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 major improvements are needed. This is specifically the case for Internal Control Principle 11 which is partially present and needs major improvements.

The major 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 by the of IT incidents that happened during 2018.

Regarding the open audit recommendations, it should be noted that improvements have already been made compared to 2017 with a 70% decrease of delayed open recommendations and that action plans for most recommendations have been approved by IAS (or pending approval) and that they are in the process of being implemented (more details in section 2.1.2.).

As for the IT incidents affecting availability and confidentiality, this will need to be tackled decisively. This calls for DIGIT to design and implement resilience into its delivery chain to ensure that digital business initiatives become sustainable operations. This will increase the ability to anticipate, prepare for, respond and adapt to change and disruptions. The first steps have already been taken (more details on page 56 onwards).

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

- IT Governance and IT security have always played and play a prominent role in DIGIT's strategic framework for the period 2016-2020 as defined in its Strategic Plan. The eleven specific objectives are grouped around five priorities, aiming at establishing and enhancing the modernisation of public administration, the digital

workplace of the future, the data centre of the future, a better IT Security, and a custom-oriented delivery of IT services (see part 1);

- The Commission's business critical activities depend even more than in the past on the availability and effectiveness of digital solutions. In 2018, there was an increase of significant IT incidents affecting both availability and confidentiality, which in light of the above dependency needs to be tackled decisively. This calls for DIGIT to design and implement resilience into its delivery chain to ensure that digital business initiatives become sustainable operations. This will increase the ability to anticipate, prepare for, respond and adapt to change and disruptions.

  DIGIT uses general procedures and processes for service management. These are based on ITIL (IT service management framework) best practices, complemented by specific rules. Security-related incidents are managed following standards of procedure defined and agreed with HR.DS1. These procedures are now being reviewed and harmonised across the organisation to create a common IT Service Management framework. A resilient ICT service needs supporting layers: these include the necessary technical and support systems, security and continuity procedures, all dedicated to providing the service according to business needs. DIGIT works on a few main streams: to create a solid, secure-by design foundation, to develop and run resilient digital business solutions and to manage risks in order to anticipate and address incidents with impact on business continuity and data protection.

- Building resilience is a process in steps. It is important to bring all these elements together to:

  - increase the ability to identify and address risks and vulnerabilities in a structured and consistent way;
  - increase coordination and integration of activities to improve coherence and performance;
  - better understand stakeholders and dependencies that support strategic goals and objectives.

  DIGIT has put in motion a series of actions to embed resilience in its delivery chain, expected to have immediate and medium term impact. DGs and business stakeholders need to adopt similar measures and work in partnership with DIGIT to ensure proper coordination. The European Commission Digital Strategy and the IT Security Strategy will drive most of these actions. The Information Technology and Cybersecurity Board needs to monitor closely the implementation of the strategies and help ensure that priorities and resources are set accordingly. DIGIT will regularly report to the Information Technology and Cybersecurity Board on the complementary resilience actions outside the scope of the strategies.

- As a result of the new data protection legislation, the Commission is faced with having to adapt processes and systems to be compliant, especially with the increased rights of data subjects, new record-keeping requirements and the new "privacy by design and by default" requirements. This latter especially has a particular impact on IT services, tools & systems. Consequently, full, smooth and timely implementation of the new rules is a challenge. It will imply increased record keeping, acquisition of expertise (legal, technical) and hiring specialised consultants.

- The conclusion of the Internal Auditor on the state of internal control in DIGIT states that the internal control systems in place for the audited processes are effective, except for the observations giving rise to the "very important" open recommendations. However, as they are addressed by action plans and are under implementation and not due yet, it does not affect the assurance.

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 but that some improvements are needed. Internal control principle 11 is considered partially effective and needs major improvements. 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 as regards assurance

This section reviews the assessment of the elements reported above (in Sections 2.1.1, 2.1.2 and 2.1.3) and draws conclusions supporting 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). 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 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 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

two 'very important' recommendations from the audit on management of IT security could have an impact, 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 improvements are needed. Internal control principle 11 is considered partially effective and needs major improvements. Considering the remedial measures already implemented (see page 57) 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 1 510 736.

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 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,

Director-General of DIGIT

In my capacity as authorising officer by delegation

Declare that the information contained in this report gives a true and fair view[28].

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, the limited conclusion of the Internal Auditor on the state of control, the observations 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 Commission.

Brussels , 29 March 2019

Gertrud INGESTAD

e-signed

[28] 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

EXAMPLE OF ECONOMY AND EFFICIENCY

As already highlighted in section 1 of this report, DIGIT is committed to optimise the management of its resources (see specific objective 11).

DIGIT also makes continues efforts to better manage its human resources, information assets and communications activities, as explained in the chapters to follow.

For more details, please refer to ANNEX 2

2.2.1 Human resource management

In 2018, the DIGIT HR BC was drafted and began implementing its HR Strategy: "HR Strategic Priorities for DIGIT", consisting of 4 main pillars:

- DIGITAL POLE in Luxembourg
- Talent scouting - Women
- Talent scouting for middle management
- Learning and Development Priorities for 2018

DIGIT invested considerable resources in increasing the percentage of female representation in middle management (HRM Indicator 1 in Annex 2). DIGIT reached in March 2018 its specific target[1] of five first appointments of women to middle management functions. This can be seen as a result of introducing the 'Talent Scouting for Women in DIGIT', a tailored programme designed to foster the development of managerial potential among female colleagues in the DG. The programme involved 20 female colleagues and proposed career guidance coaching, group coaching, preparation for interviews, lunchtime talks, and specific training paths. It also promoted the creation of a supportive network among female colleagues.

In regards to the overall staff engagement index and the percentage of staff who feel that the Commission cares about their well-being (HRM indicators 2 & 3 in Annex 2), DIGIT continued to roll-out concrete actions for addressing the decrease of scores – and underlying deficiencies - in the 2016 Staff Survey. In 2018, DIGIT offered to its staff workshops and information sessions on better ways of working in open space, promoted a more flexible teleworking culture, launched an internal mobility call and implemented more transparent management communication through weekly interactive video debriefs of the management meeting. The results of the staff survey 2018 confirmed that the measures put in place contributed to reaching the targets of indicators 1, 2 & 3.

For an extensive reporting on all the above components, please refer to Annex 2.

[1] SEC(2017)359: "Quantitative targets of first female appointments to be made per Directorate-General and service at middle management level by 1 November 2019"

2.2.2 Information management aspects

The document management function is well established in DIGIT, as shown in Annex 2.

In 2018, DG DIGIT Senior management addressed data protection on several occasions to prepare for the entry into force of the revised Regulation on data protection (EU (2018) 1725). It carried out an internal stocktaking to identify all processing operations handling personal data. These operations were then assessed for compliance with the general principles of the revised legislation and remedial actions initiated where necessary. In alignment with the recommendations of the Commission's Data protection Officer, priority was given to ensuring compliance of those processing operations involving the general public e.g. outward facing web sites.

With the adoption of the Commission's Data Protection Action Plan in November 2018, DG DIGIT also began an examination of how to strengthen its administrative capacity for dealing with data protection issues and in particular the implementation of the above-mentioned action plan in 2019.

2.2.3 External communication activities

In 2018 DIGIT updated its Communication strategy (''Dream DIGITal – DIGIT Communication strategy 2018-2020''). In line with the Strategic Framework 2016-2020, DIGIT has an enhanced external communication role in supporting projects addressing EU citizens (e.g. ''Connected Digital Single Market'') as well as an increased focus on attracting the best talent. In 2018 the external communication activities were focused on:

1. A stronger branding and user-centric culture reflected in DIGIT's public web presence through social media campaigns activities. The Cyber Security Month in October 2018 was among the campaigns with the biggest impact on social media. It was implemented in collaboration with DG CNECT, DG COMM, DG HR and ENISA.

2. Improved coordination between all actors involved in the external communication activities in DIGIT:
   - through the regular meetings of the External communication network in DIGIT
   - through the regular meetings of DIGIT representatives in the coordination of campaigns with DG CNECT, SPP and Cabinets

3. DIGITEC conference, jointly organised by DIGIT and the IT departments of the European Parliament and the Council of EU on 20th of November 2018, was coordinated by DIGIT communication team working closely with teams from all DIGIT directorates. The co-created event is where Commission's achievements in digitalisation are showcased to the EU staff, partner organisations and through webstream – to the larger EU public. It is also the only large-scale event for the IT communities of the EU institutions to exchange best practices and to network.

4. Cybersecurity – in the context of its corporate Cyber Aware program, DIGIT has organised a Women in Cyber event on 8th of March 2018, hosted by Commissioner Mariya Gabriel and with participation of representatives of leading IT companies and non-for-profit organisations working to bridge the gender gap in cybersecurity. The event was publicly webstreamed and covered on social media. A similar event was organised in the context of the Cyber Week in Luxembourg on the 12th of October 2018.