EUROPEAN COMMISSION CLOUD STRATEGY

Cloud as an enabler for the European Commission Digital Strategy

16 May 2019

V.1.0.1

Informatics

Table of Contents

1. EXECUTIVE SUMMARY

The European Commission Digital Strategy (ECDS) sets a vision for a digitally transformed, user focused and data driven administration by 2022. This ambitious goal requires transformational changes in a number of key area, with IT transformation supporting the business transformation.

One of the enablers of this transformation of IT is Cloud computing. This new paradigm of IT service delivery has brought two key changes to the IT landscape.

- One is a global market place of IT services that allows on-demand consumption of IT resources, advanced IT building blocks and even complex business applications without investing in IT infrastructure.
- The other is a new way of developing information systems (cloud-native) based on these cloud-based IT services. This allows a reduced complexity of the information system and instead an increased focus on the business value. Together these two changes enable the transformational change of IT to support the business transformation.

The European Commission has promoted Cloud Computing towards companies and public administrations alike since the adoption of the first European Cloud Computing Strategy[1] in 2012. In line with European cloud policies towards government authorities, DIGIT has pioneered the experimentation of Cloud computing by the EU Institutions and agencies and has distilled the experience in a comprehensive list of lessons learned.

The experience has confirmed the transformational potential of Cloud computing, but also shows that corporate governance and security management require special consideration to avoid unwanted exposure to risks in the area of costs and information security.

Based on these lessons learned, the European Commission defines a vision for Cloud computing:

Cloud-first with a secure hybrid multi-cloud service offering

Cloud-first means that systems should rather be conceived in such a way that they can benefit from the advantages of cloud based delivery models, which exist both on premise and in the public cloud. The choice of architecture, especially of on premise and/or public cloud, will depend on the advantages, constraints and risks for a specific system. So it does not mean that all systems should go to the public cloud.

The **Cloud-first** approach implies that any new development should preferably be cloud-native, and existing information systems should be reassessed for transformation, rewriting or replacement within the context of the modernisation plans foreseen by the European Commission Digital Strategy, seizing the opportunities arising in the business and application lifecycle.

The Cloud service offering available to the European Commission must be:

- **Secure** by identifying and managing IT security risks and handling data in line with its classification, as well as compliant with **data protection** obligations of the European Commission;

[1] COM(2012) 529 Unleashing the Potential of Cloud Computing in Europe

- **Hybrid** by utilizing services both from public cloud providers as well as an on premise European Commission managed private cloud;
- **Multi-cloud** by not tying the European Commission to one public Cloud provider and source from the cloud provider best suited to provide the requested service;
- **Energy-efficient** in line with the overall EU priority of lowering carbon footprint and with green public procurement policy.

To implement this vision, changes are needed in a number of key areas:

In the area of **IT Governance**, the European Commission will, in the context of the Governance package adopted in November 2018, revisit the governance processes for the lifecycle of information systems and make sure that they are fit-for-purpose to handle all aspects of cloud computing. Additionally, it will put in place the necessary mechanisms to ensure that the modernisation roadmaps required in the context of the European Commission Digital Strategy are aligned with cloud-first principles.

The governance of cloud-specific risks will be supported by a new tool, GovSec, offering hands-on risk management support for cloud-based systems. The tool will enable a practical and common approach towards managing the cloud risk landscape, saving valuable time during the mandatory risk assessment phase of projects, while also assuring a common baseline across the European Commission, Institutions and agencies.

DIGIT will continue to operate as Inter-institutional Cloud Broker, in order to enable the European Commission and interested European Institutions and agencies to efficiently and safely procure Cloud services from a broad range of Cloud service providers, mitigate the risk of vendor lock-in, facilitate cost monitoring and forecasting and provide guidance. For the European Commission the Cloud Broker will also deliver foundational cloud services and enforce a common baseline of security and data protection across all cloud usage.

In the area of **Digital Solutions**, the European Commission will favour the sourcing of generic or standard solutions from the market of cloud-based business applications (Software as a Service). For policy specific solutions, the European Commission should promote a shift to Cloud-native development methodologies, a change that requires a transformation of mind-sets, processes, architecture and technology.

In the area of the **Reusable Solutions Platform**, the European Commission will transform existing services, frameworks, building blocks and technical platforms to cloud-native services within a comprehensive Reusable Solutions Platform.

In the area of the **Data Ecosystem**, the European Commission will transform into a data-driven organisation by setting up a data ecosystem for capturing, curating, storing, protecting, elaborating, accessing, using, re-using, consuming, analysing, disseminating and sharing data.

In the area of the **Digital Workplace**, DIGIT will leverage a hybrid cloud SaaS platform to provide the European Commission with a digital workplace environment that enables users to work and collaborate anywhere and anytime from any corporate device.

In the area of **Digital Infrastructures**, DIGIT will provide Hybrid Cloud services to the European Commission and interested institutions and agencies. To achieve this goal, it will create a Hybrid Cloud solution architecture service and transform its Data Centre services to Hybrid Cloud services, built on top of both public and on premise private Cloud infrastructures.

In the area of **Cloud Security Services**, DIGIT will provide to the European Commission cloud-enabled security services for all phases of the lifecycle of all types of consumption of Cloud services.

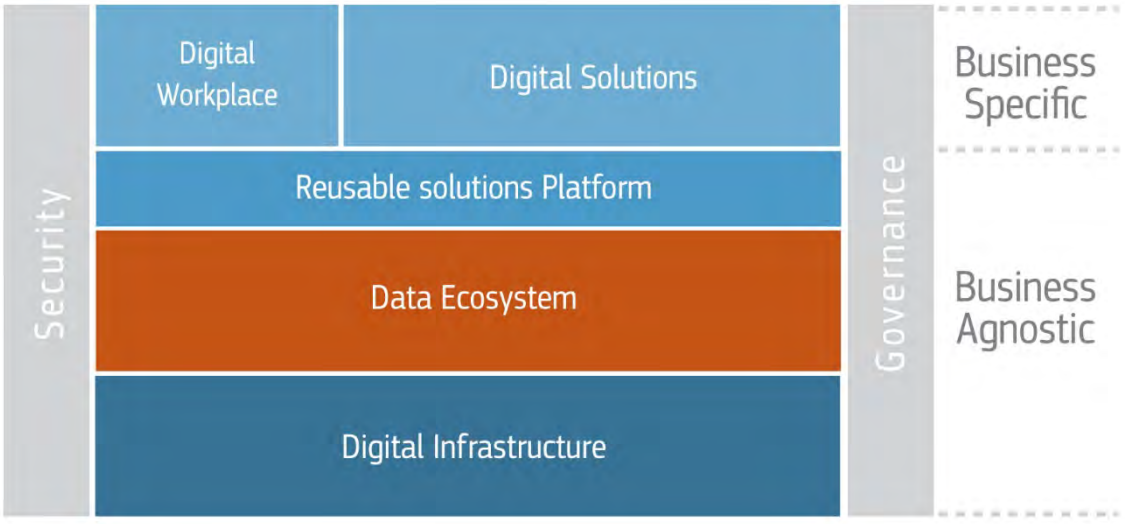
2. INTRODUCTION

2.1. Context

The European Commission Digital Strategy, adopted on November 21st 2018 by the College, sets a vision for the Commission to become a digitally transformed, user-focused and data-driven administration by 2022.

> By 2022, the Commission will be a digitally transformed, user-focused and data-driven administration — a truly digital Commission. It will be endowed with a new generation of trusted and personalised digital solutions supporting its digitalised policies, activities and administrative processes. These solutions will increase the Commission's efficiency, effectiveness, transparency and security and will deliver EU-wide, borderless, digital public services that are indispensable for the functioning of the European Union.

To achieve this ambitious goal, the European Commission will need to undergo a number of transformations in key areas.



This document outlines a Corporate Cloud Computing Strategy that aims to fulfil the transformational requirements that the Digital Strategy places on IT itself.

2.2. Cloud computing

"Cloud computing" is an IT paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level IT services that can be dynamically provisioned with minimal management effort, usually over the Internet. Cloud computing relies on the sharing of resources to achieve coherence and economies of scale, similar to a public utility.

The key characteristics of cloud computing are that IT resources are provided on-demand in an "*elastic*" way (i.e. they scale up or down dynamically to meet fluctuating demand), the service is *metered* (you only pay for what you actually consume) and services are requested through a "*self-service*" online control panel.

Cloud computing has quickly created a global marketplace. Initially focused on IT resource provisioning (Infrastructure as a Service, IaaS), the market has also quickly expanded to provide

advanced IT services such as databases and analytics (Platform as a Service, PaaS) and also business applications (Software as a Service, SaaS). Due to the global scale of the marketplace, many services are available for consumption, and as all of these services are small and scope-limited, many more are continuously created.

This global marketplace of Cloud services has sparked the creation of a new transformational programming paradigm, where cloud-native information systems are built on top of a combination of cloud based services, independent of the underlying IT infrastructure.

With code being written at a much higher abstraction level, the amount of code needed for the same functionality gets reduced significantly. This smaller code base decreases operational costs, increases agility, enables faster rewrites to adapt to changes and reduces the maintenance efforts. All of this allows the business to spend more time on business matters instead of IT matters.

3. THE EUROPEAN COMMISSION'S CLOUD EXPERIENCE

3.1. The road so far

In September 2012, the Commission adopted the European Cloud Computing Strategy which called upon member states to embrace the potential of cloud computing. It was observed that "the economic impact of cloud computing will not reach its full potential unless the technology is adopted by both public authorities and small to medium sized enterprises (SMEs)".

DIGIT's first Cloud strategy was approved in May 2014 and received full support of the ABM+IT Steering Group on 22 July 2014. It outlined a path towards a diversified IT infrastructure landscape that consisted of traditional IT and more modern cloud computing based IT. It defined the governance framework required to acquire and use cloud resources in a secure and policy-compliant manner.

To enable and assist all European Institutions on this journey, DIGIT launched an inter-institutional Call for Tender for Cloud Services (Cloud1) in December 2014. Due to the innovative way of tendering, it took until December 2015 to sign the first contracts with the winning tenderers.

A number of institutions and Commission DGs decided to use Cloud1 for their information systems. DIGIT created two parallel tracks: an experimental track that was aimed at gaining as much experience as possible with cloud technologies, and a Data Centre track to explore how cloud-based IT services can be provided in a secure manner with long-term sustainability.

3.2. Lessons learned

DIGIT has continuously monitored progress on both tracks and has collected feedback from all Cloud1 use cases. A number of information systems are today benefiting from cloud resources and several services are natively provided via cloud resources. This has allowed the European Institutions to learn a number of important lessons:

(1) The ubiquitous availability of business applications for consumers has dramatically changed their expectations of corporate IT solutions. Like Cloud solutions, corporate IT must be accessible anywhere, anytime, from any (corporate) device.
(2) Not all Cloud deployment models (especially off-premise private Cloud) can provide the functionality and benefits required by the European Commission.

(3) The global marketplace of Cloud services is growing rapidly and offers innovative services ready for consumption for IT consumers or IT architects.
(4) The elasticity of Cloud services and the pay-per-use model allows Cloud-native information systems to deal with significant peaks in resource consumption without service degradation at a reasonable cost point.
(5) Only Cloud-native information systems can fully benefit from Cloud computing. Existing information systems can be made to profit from some aspects of Cloud computing, but will never be able to reap all possible benefits.
(6) Cloud-native information systems are an enabler for data-driven organisations to exploit significant data volumes for the benefit of its customers.
(7) The usage of Cloud services allows the European Commission to benefit from security services operating at a global scale and thereby reduce corporate IT risks.
(8) The lifecycle of an information system must be closely managed to ensure that security concerns are proactively addressed at all stages.
(9) The diverse sources of Cloud services allow the European Commission to increase its business-continuity resilience by reducing the dependency on individual suppliers.
(10) Cloud computing is a new paradigm that is significantly different from how IT has worked so far. The split of responsibilities between information system owners and the various actors working on their behalf (architects, developers, operations) is therefore shifting, putting more responsibilities on the information system owners.
(11) At the same time, existing IT skills do not translate very well to cloud computing. A number of new roles need to be filled and Cloud-native technologies like Infrastructure as Code require very different profiles. Competition for all of these cloud-enabled profiles is fierce, which obliges the information system owner to fill a significant skills gap.
(12) Inter-institutional cooperation between the European Institutions and agencies provides economy of scale benefits for all participating entities.
(13) The availability of business applications in the Cloud creates huge opportunities for business users while challenging existing corporate risk management and governance processes.
(14) Portability and reusability of information systems must be controlled to manage dependencies on particular Cloud Service Providers.
(15) The inherent risks of cloud due to the discrepancies of European and American legislation can and must be mitigated when dealing with global cloud providers, inter alia through a combination of vendor due diligence, contractual provisions and technical security controls.

A more detailed description of these Lessons Learned can be found in Annex 1.

4. VISION

Cloud-first with a secure hybrid multi-cloud service offering

Cloud computing is an industry-wide game changer that will shape the IT landscape for the foreseeable future. The European Institutions have gained enough experience with the opportunities and pitfalls of Cloud computing to understand that Cloud computing is an important and necessary enabler to implement the transformation goals outlined in the European Commission Digital Strategy.

While it is possible to quickly derive some limited benefits of Cloud computing by moving existing information systems to use Cloud resources with sometimes only minimal modifications ("lift and shift"), the real value of Cloud computing can only be unlocked by moving information systems to a cloud-native development pattern. This is easier to achieve for new information systems, but will require a more fundamental transformation for existing ones, our IT legacy. IT teams must start employing agile and cloud-native development practices like DevSecOps, and design systems according to modern data-centric architectures supporting the consumption of loosely coupled micro-services. It is therefore essential to adopt a **Cloud-first approach**: Any new development should preferably be cloud-native, and existing information systems should be reassessed for transformation, rewrite or replacement in the context of the digital solutions modernisation plans foreseen by the European Commission Digital Strategy.

Cloud-first does not mean that all systems should go to the public Cloud. It means that systems should rather be conceived in such a way that they can benefit from the advantages of cloud-based delivery models regardless of whether the data or processing capabilities are on premise or in the public cloud.

This brings us to the second pillar of the cloud strategy: **hybrid**. The amount of data processing that is happening today and will happen in the future will require an ever-increasing decentralisation of data and compute resources. As a first stepping-stone into such a future, Cloud resources with the appropriate levels of encryption and access control have proven themselves to be viable for the majority of information systems that do not process classified information. Nevertheless, a number of information systems processing non-classified information have properties that for technical or political reasons require the privilege and immunity protection of Article 343 of the Treaty on the Functioning of the European Union (TFEU). For these use cases, it is important to offer Cloud services that run on the premises of the European Commission. It is therefore required to work with a **Hybrid** Cloud setup and utilise IT services from public cloud providers as well as services provided by an on premise EC-managed Cloud. This way of working will become the new delivery model for the European Commission's data centres, fully automated and with systems segregated by default in order to provide a higher level of cyber-protection than in the current data centre setup. Based on their security needs, data classification and data residency requirements, information systems and their associated data will be placed in the appropriate facilities, either in the on premise private cloud or in the public cloud.

Cloud services must be designed and operated according to security best practices. Legacy IT security controls don't necessarily align with these cloud best practices. Identifying the resulting IT security risks, managing them over the full lifecycle of an information system and ensuring compliance with mandatory requirements like data residency is a governance challenge essential to **securely** run cloud-native information systems at scale.

Cloud providers have strengths and weaknesses in different areas. Tying the European Commission to a single provider means that the architects of new information systems would only be able to utilize a reduced set of Cloud services. The European Commission should therefore choose a **Multi-Cloud** approach and not tie itself to one public cloud provider. Depending on the use case, the European Commission will source its IT services from the cloud provider that is best suited for the service required.

5. GOVERNANCE

5.1. Governance of the information system Lifecycle

Our lessons learned show that the usage of cloud services can bring significant rewards, but at the cost of new types of risks. The security and integrity of information systems using cloud services depends on the proper identification and management of these risks and the implementation and maintenance of appropriate security measures during the whole lifecycle of an information system.

With the recently implemented "governance package", corporate IT and Cybersecurity governance falls under the responsibility of the newly formed Information Technology and Cybersecurity Board (ITCB), whereas the corporate governance of data happens in the Information Management Steering Board (IMSB).

The relevant Commission IT governance bodies, ITCB and IMSB, will ensure that all legal requirements, security principles and best practices with regards to the usage of cloud services are embedded in the lifecycle of information systems.

Commission Services have to comply with Commission Decision (EU, Euratom) 2017/46, and the forthcoming "Principles and rules for outsourcing of communication and information systems".

The secure and safe usage of Cloud services is intrinsically linked to an appropriate data classification for all data assets of an information system. It is imperative to make sure that information security rules are applied in all usage of Cloud services whether on premise or in the public cloud, and especially when business applications are consumed as Software as a Service. In particular, EU Classified Information (EUCI) is not suitable for either mode of cloud provisioning. The risk assessment should take due account of the handling of sensitive but not classified (SNC) information in both private on premise and public cloud.

Aspects that will be monitored in particular are:

- The exclusive use of the forthcoming DIGIT cloud framework contract (Cloud II) and the DIGIT cloud broker service[2], establishing a minimum common baseline for procuring cloud services efficiently and securely;
- Outsourcing activities must be recorded and kept up to date in the corporate IT portfolio management system (GovIS2);
- Appropriate and adequate risk assessments is done (inter alia a Data Protection Business Impact Assessment and IT Security Risk Assessment) prior to deployment in

[2] See section 5.4 below

the public cloud and each time there are changes that have a significant impact on the risks[3];

- The application of relevant data classification rules[4] and identification of data localisation requirements is followed;
- "Commission Use" (CU) and "Sensitive Non-Classified" (SNC) information must geographically reside on European territory;
- Compliance with the rules and guidelines for the protection of personal data[5];
- Evaluation of business continuity measures in particular data and IT asset portability, including the ease of switching of cloud service providers;
- The completion of a security plan together with an evaluation of security and business continuity measures and an assured follow-up and monitoring of these measures.

The European Commission will apply all legal requirements and best practices for the lifecycle of information systems within the corporate IT governance framework that supports all aspects of cloud-based information systems.

5.2. GovSec – A common platform for cloud risk management

A practical and common approach towards managing the risk landscape is an essential enabler for achieving the aforementioned governance objective for safe cloud adoption. In this context, DIGIT is developing the GovSec tool, which will offer hands-on risk management support for cloud-based systems.

GovSec will facilitate the dissemination of secure cloud deployments through a common risk and corresponding mitigation database. A common risk landscape database avoids that system owners have to start each risk analysis from scratch, a time consuming and inefficient process, but instead can build upon a shared registry already tackling generic, recurring risks associated with the cloud services used.

Hence, system owners can focus on the specific, residual risks for their use cases, while benefiting from generic solutions for generic, pre-identified risks. Such an approach not only saves valuable time during the mandatory risk assessment phase of a project, but it also assures a common baseline across the European Commission, Institutions and agencies.

GovSec will support the three areas where cloud consumers have to demonstrate compliance: i) Risk Assessment (sustained by the ITSRM² methodology); ii) Decision making and Governance; iii) Implementation (i.e. support for Security Plan).

The Decision & Governance module will provide a standard and customisable approach to accompany system owners in their cloud journey: it invites to reflect on hosting options, classifying business data, and defining at a business level where and how this data should be managed. This simple and straightforward methodology helps to structure the debate that must take place in any cloud adoption process.

[3] In conformity with the internal data protection Regulation (EU) 2018/1725 and the use of ITSRM[2] and its associated threat catalogue.

[4] Security Notices C (2019) 1903 and 1904

[5] Regulation (EU) 2018/1725 and EDPS guidelines, including "EDPS Guidelines on the use of cloud computing services by the European Institutions and Bodies, 16 March 2018"

The GovSec Risk Assessment and Implementation modules implement the ITSRM2 methodology. Its catalogue will be gradually extended with cloud specific threats like vendor lock-in, loss of governance, isolation failure, management interface compromise, insecure or ineffective deletion of data, compromise of service engine, subpoena and e-discovery, risk from changes of jurisdiction, data protection risks, accountability and data ownership, user identity federation, user privacy and secondary usage of data, incident analysis and forensic support or insecure interfaces and APIs.

The risk assessment module output is a series of mitigation measures translated in technical implementations that can be monitored in the context of a security plan. The main advantage of the approach is consistency between mitigation measures, which are often high-level, and the technical measures to be implemented and are part of Implementation Module.

GovSec specifically caters for the shared responsibility model, where cloud providers can contribute to the risk assessments of their services. Based on this information, system owners can see to which risks they are exposed, which mitigations the cloud suppliers already have in place and what is the remaining part that needs to be covered.

GovSec will open a new set of capabilities in the domain of cloud risk management: easy maintenance of risk assessments and security plans, increased consistency of risk assessments and the automation of risk assessment updates when services are modified.

DIGIT will develop a tool offering hands-on risk management support for cloud-based systems. The tool will enable a practical and common approach towards managing the cloud risk landscape, saving valuable time during the mandatory risk assessment phase of projects, while also assuring a common baseline across the European Commission, Institutions and agencies

5.3. Transforming the portfolio to cloud-native digital solutions

In the context of the digital modernisation plan outlined in the European Commission Digital Strategy, existing information systems will need to be brought into the Cloud era. This forces the European Commission to review its portfolio of information systems via modernisation roadmaps to be reviewed and approved by corporate IT governance.

Possible modernisation strategies are:

- Rehost: Lift-and-Shift the existing information system to the Cloud without adapting it (whether on premise or in the public cloud);
- Refactor: Rebuild problematic components to better fit into Cloud environments;
- Rebuild: Re-architect the information system as cloud-native information system;
- Replace: Replace the information system with a Software as a Service business application.

These different modernisation strategies all have their advantages and disadvantages and the choice of modernisation strategies need to take them into account as much as certain core properties of the information system to be modernised (business value, business criticality, age of the information system, information classification, …).

The guiding principles for this cloud transformation are the following:

1. **Business driven**: DGs will transform as needed their application portfolio, consolidating, re-architecting or re-platforming then into a cloud-native paradigm within the context of the European Commission Digital Strategy.

2. **Opportunistic, lean and agile**: The modernisation will be executed over several years, aligning with the opportunities arising in the business and application lifecycle in order to avoid unnecessary expenses. Given the rapid changes in the technology, projects should follow a lean and agile approach.
3. **Saas > Paas > Iaas**: When modernising or renewing applications, Software as a Service will be targeted in preference for generic or standard functionality, while Platform as a Service and, as a last resort, Infrastructure as a Service are natural targets for policy-specific solutions.
4. **Strong foundation**: The foundational elements and common services, including architecture blueprints, identity management, monitoring and security will be provided by DIGIT. This will assure both coherence and compliance with security and data protection obligations at a corporate level.

Portfolio management needs to ensure that dependencies between information systems are taken into account when drawing up the individual modernisation plans. It must also help with prioritizing investments and providing input for the necessary Reusable Building Blocks and Infrastructure Services required to enable the goals of the European Commission Digital Strategy.

In the context of the EC Digital Strategy, information system owners will create modernisation roadmaps for their information systems that are aligned with the Cloud-first strategy and the four guiding principles for cloud transformation, and present them to the corporate governance bodies for approval.

5.4. DIGIT as Inter-institutional Cloud Broker

A key goal of procurement in the context of Cloud computing is to ensure continuity of service. Poorly managed cloud contract transitions, can potentially stop all operations and lead to a loss of data.

Moreover, Cloud technologies evolve daily. New services with high potential (i.e. in the field of Artificial Intelligence) appear suddenly and are constantly evolving. A second procurement objective is therefore to ensure access to a broad variety of evolving Cloud technologies.

Procurement must be an enabler in the usage of Cloud resources. DIGIT will define suitable procurement solutions (Framework contracts, Dynamic Procurement System) to ensure continuity of service and the widest possible access to the market, including European SMEs.

The procurement strategy for Cloud envisages the role of a centralized inter-institutional broker, which enables stronger leverage from Institutions on the public Cloud market. This leverage allows the Institutions to:

- Negotiate better terms and prices in the scope of this contract
- Impose to the extent possible, contractual modalities in line with the EDPS “Guidelines on the use of cloud computing services by the European Institutions and Bodies”, like:
  - ✓ Data and assets must geographically reside on European territory
  - ✓ Algorithms and analytics must also be run in Europe
  - ✓ Providers must accept audits from the main EU bodies
- Enforce a common baseline of **security** and **data protection** across all Cloud usage to mitigate the inherent risks of cloud as described in the “Lessons Learned” section.
- To the best of our capacity, influence the technical roadmap of providers

- Impose specific energy-efficiency objectives for cloud services (Green Public Procurement)
- Ensure the respect of self-regulatory Codes of Conduct established by the industry[6]

Since 2015, DIGIT has already acted as Cloud Contract Broker for DGs, Institutions and agencies. DIGIT manages a common Framework contract for Cloud services, facilitates the execution of specific contracts and delivers expertise to its customers on request.

DIGIT will continue to play the role of Inter-institutional broker by delivering common framework contracts for the benefit of the Institutions and offering its services as a contract broker to participating Institutions and agencies.

It is important that the European Institutions continue to have a single point of presence on the Cloud market. Only by acting as a single entity will the European Institutions have the necessary leverage on the market to impose necessary specific terms, for instance in the areas of auditing and data residency or data protection in general.

However, for the European Commission, DIGIT's role as cloud broker cannot be limited to procurement. DIGIT must also provide value-added cloud foundation services. Such services include architectural guidance (e.g. validated and tested blueprints and patterns), Cloud-compatible and secure identity and access control, centralised log management, alerting and monitoring (in particular with regards to cost control) and security services such as monitoring, prevention, detection and incident response.

DIGIT will continue to operate as Inter-institutional Cloud Broker to enable the European Commission and interested European Institutions and agencies to efficiently and safely procure Cloud services from a broad range of Cloud service providers, mitigate against vendor lock-in, facilitate cost monitoring and forecasting and provide guidance. For the European Commission, the Cloud Broker will also deliver foundational cloud services and enforce a common baseline of security and data protection across all cloud usage.

6. DIGITAL SOLUTIONS

Section 5.3 focused on the cloud-native transformation of the European Commission's existing application portfolio. However, the transformation to a truly digital Commission requires the European Commission to invest also in a new set of trusted digital solutions. This transformation applies not only to the functionality of the digital solutions, but also to the way that they're being envisaged.

On the one hand, for generic or standard solutions, the Commission must embrace Software as a Service buying generic services on the market, for which it does not make sense to do in house development. On the other hand, the European Commission will also need to continue to invest

[6] The European Commission is facilitating self-regulatory work from industry to develop recommendations for the purposes of a European Cloud Certification Scheme. Such scheme has the potential to facilitate the free movement of data, enable a better comparability of cloud services and promote cloud uptake. The Commission may request the European Union Agency for Network and Information Security (ENISA) to prepare a candidate scheme in accordance with the Cybersecurity Act's provisions. Such scheme will address both personal and non-personal data and will thus also provide an assurance on implementation of security measures. At this moment, several codes of conducts have been established by the industry, for instance by the Cloud Select Industry Group (C-SIG), the Cloud Infrastructure Service Providers in Europe (CISPE) and the Cloud Security Alliance.

in policy-specific solution development, switching to a Cloud-native development process. This requires a deep cultural transformation of the lifecycle of information systems, focusing on mind-sets, processes, architecture and technology.

Cloud-native development starts by reinforcing the relationship between development, operations and security teams by fostering collaboration. This is enabled by putting in place solid DevSecOps practices. This requires a cultural shift where developer teams care about how their digital solutions run in production and where operations teams know how the digital solutions work.

Cloud-native solutions require new architectures which combine a data centric approach with the consumption of Cloud services. Monolithic information system architectures need to be replaced by distributed architectures where an orchestration layer combines self-contained functional micro-services and data repositories. By using Cloud services wherever possible, the footprint of these components can be significantly reduced, enabling more agility for the DevSecOps processes.

Service reusability must be the leitmotif for cloud-native development. New projects will first search and select the existing micro-services they need to rely upon, and build their own micro-services only in areas that are not covered. This again reduces the footprint of information systems. In an ideal case the information system consists of a User Interface with minimal glue code that links existing micro-services together.

DIGIT will publish a cloud-native reference architecture that contains relevant architecture patterns and guidelines. DIGIT will identify the tools and products necessary to enable cloud-native development and will deliver associated services to facilitate their adoption inside the Commission. DIGIT will provide guidance around best practices in cloud-native development based on agile DevSecOps.

For generic functionality, the European Commission will favour cloud-based business applications (Software as a Service) over in-house development.

For policy specific solutions the European Commission embraces a shift to Cloud-native development methodologies, a change that requires a transformation of mind-sets, processes, architecture and technology.

7. REUSABLE SOLUTIONS PLATFORM

The Digital Strategy encourages the development and reuse of business agnostic "reusable solutions", which can take different forms: common (managed) services (Commission Notification System, Enterprise Search, etc) frameworks (eUI, mobile apps, etc), CEF building blocks (EU Login, EU SEND, EU SIGN, etc), more sophisticated technical platforms (Compass Corporate), etc. The approach is to identify the various existing reusable solutions, which have different maturity levels, and to progressively integrate them in a consistent platform (the Reusable Solutions Platform) offering a standardized service for each of them: proper governance, definition in a harmonised catalogue of service, documentation, support, service level agreements, key performance indicators, cost-model, etc.

The setting up of the platform itself entails tackling several challenges, from definition of the solution portfolio (what Reusable Solutions are part of the platform) and governance/funding, to cartography (which information systems need which reusable solution), setting up a proper service (document, support, helpdesk, operations), while striving for the highest quality.

The cloud approach (full automation, elasticity, pay per use, variety of state-of-the art services, containers and orchestrators, etc) is particularly well suited for Reusable Solutions which are meant to be shared by as many systems as possible, developed independently from each other and by different teams but respecting the same architectural standards, promoting micro-services rather than monoliths, and relying on an agile DevSecOps approach to quickly adapt to the needs of the information systems consuming them.

The Commission also aims at playing an active role in offering European Public Administrations cloud services for enabling government interoperable data platforms and services. The CEF Big Data Test Infrastructure, a first implementation of such a cloud service, has already gained traction for a number of specific test implementations. Similarly, the Interoperability Test bed offered by the ISA^2 program is providing a cloud service to European Public Administrations for interoperability and conformance testing facilities.

The European Commission will transform existing services, frameworks, building blocks and technical platforms to cloud-native services integrated within a comprehensive Reusable Solutions Platform.

8. DATA ECOSYSTEM

The European Commission data strategy, which is in integral part of its overarching digital strategy, aims at transforming the institution into a data-driven organisation by setting up a data ecosystem, i.e. a system of resources and services for capturing, curating, storing, protecting, elaborating, accessing, using, re-using, consuming, analysing, disseminating and sharing data.

The EC data ecosystem will rely on a technical infrastructure able to cope with a modern way of managing data. Cloud based solutions represent the reference for handling (big) data, the associated services and analytics.

An organic development of data centric information systems and related services relying on hybrid cloud infrastructure which adequately take into consideration data protection and security is paramount for the achievement of the targets of the DataStrategy@EC Action Plan.

The roll-out of the EC data strategy will set up the foundation for enabling modern data management and the provisioning of services, including Data as a Service (DaaS), through the data platform. This will enable the EC data ecosystem to be deployed on the hybrid cloud.

The European Commission will transform into a data-driven organisation by setting up a data ecosystem for capturing, curating, storing, protecting, elaborating, accessing, using, re-using, consuming, analysing, disseminating and sharing data.

9. THE DIGITAL WORKPLACE: TOWARDS A HYBRID CLOUD PLATFORM

The consumerization of IT has dramatically reshaped the expectations of today's corporate IT user. The requirements to be able to work anywhere, anytime, from any (corporate) device and collaborate efficiently with a growing number of internal and external stakeholders place constraints on the office automation tools that cannot be fulfilled without a transformation towards a cloud-native setup. DIGIT has started this transformation in 2017 with the Digital Workplace (DWP) Program.

The goal of the DWP Program is to provide the right IT tools, platforms and services, enabling users to work and collaborate anywhere, anytime with a fit-for-purpose security and optimizing their work experience and productivity. It is adaptive and flexible to incorporate different types of users, new behaviours and new technologies.

The main drivers for a strong Cloud strategy for the DWP are:

- **The market shift towards business applications (Software as a Service):** Five to ten years from now, the possibility exists that none of the main vendors will continue to support on premise solutions. It's therefore important to select suppliers that offer hybrid solutions, where service infrastructures can be stretched across on premise parts and the cloud, in a transparent manner for users. Today, the cloud-based business applications offering is already much richer and offers new and powerful tools demanded by users. Market investment from key vendors is always done on a cloud-first basis.
- **The increase in demand and scope of services:** This involves also an increasing need of exchanging, collaborating, creating content with increasingly larger and numerous communities outside our institution. This requires an elastic and efficient infrastructure, with strong *Data Analytics*, *Business Intelligence* and *Artificial Intelligence* solutions, which cannot be delivered on premise in an efficient and cost effective manner.

These two drivers show that a strong Cloud strategy for delivering digital workplace services is not only a **necessity**, but also an **opportunity**.

The vision of the DWP was established in 2017 to cover the needs of our internal workforce. Today, it is clear that our staff is increasingly collaborating with external communities either in the development of EU programmes and policies, or in their execution. The lack of integrated IT reaching out to these external communities tools is becoming an impediment. This requires the extension of the DWP vision to cover not only staff but also the communities and stakeholders we collaborate with. This is only feasible with a strong Cloud component, as it requires the need for a highly elastic, cost effective and secure setup.

The Digital Workplace Program is based on a **hybrid infrastructure**, mixing on premise and online (Cloud) services. The basic principles underlying this infrastructure are that it is:

- **transparent for users** – users should be able to work, collaborate and exchange information irrespective of its location (on premise or in Cloud)
- **cyber-secure and compliant with the applicable Data Protection regulation** – systems secured from an established Root of Trust with additional and efficient safeguards must be in place to cover all risks without burden on users
- **optimized in terms of overall costs** – choice of Cloud services or online services are selected to keep costs as low as possible within the limits imposed by security measures
- **flexible in terms of adoption of new online services** – to benefit from the rapid evolution of the Software as a Service offering on Cloud
- **elastic in terms of usage** – to allow rapid increase of demands when needed, within the cost limits

The DWP program has been structured in 6 different strands:

- **Devices** which need to be connected everywhere and at any time, requiring online (Cloud) services for their connectivity outside the perimeters of the institutions buildings and network

- **Office Automation** for the creation and editing of documents, where Cloud-based tools can be used to extend collaboration towards external communities
- **Mail & Calendaring**, for exchanging information and organizing worktime.
- **Unified Communication**, for real-time communication, with Cloud based solution to bridge towards external communities, including EU delegations across the world
- **Collaboration tools**, for co-creation and editing and exchange of content, again with Cloud based components to collaborate with external communities
- **Identity & Access Management**, to ascertain and protect the identity of users. This I&AM solution must integrate the use of Cloud and on premise services and assets in a seamless and secure manner under the ownership of the European Commission

The use of Cloud services including tight collaboration with external communities require that we strengthen security measures:

- Using **Digital Rights Management, strong authentication and access** techniques (based on an I&AM solution under the ownership of the European Commission, i.e. EULogin) to avoid the leaking of information and documents outside groups and people to whom its access is allowed.
- Developing and enforcing the necessary security and data protection policies. These policies should define in particular what assets or services are accessible by whom (internal or external), according to which rule and also where specific types of data should be stored (on premise or on Cloud) and how they should be protected.
- **The continuous development of our DWP Hybrid platform**, in compliance with the security and data protection policies, but also following the technology evolution.
- **The development and evolution of our support services** to encompass the DWP Hybrid Cloud concept and serving all user communities.

In line with the above mentioned principle that for standard functionality the European Commission will favour Software as a Service, the core functionality of the future DWP office automation environment will be based on a best-of-breed SaaS platform. However, this SaaS platform will be operated in a hybrid setup, on the one hand, providing the benefits of cloud solutions such as agility, value for money, security, performance and resilience, while at same time providing dedicated “on premise” protection for our most critical information assets. The proposed solution will be subject to a security risk and a data protection impact assessment in order to provide assurance with regards to information security and the proper treatment of personal data.

DIGIT will leverage a best-of-breed SaaS hybrid cloud platform to provide the European Commission with a digital workplace environment that enables users to work and collaborate anywhere and anytime from any corporate device.

10. DIGITAL INFRASTRUCTURE

In order to be able to provide the hybrid Cloud services that the European Commission needs, the Digital Infrastructure services of DIGIT will need to change along three axis:

(1) A Hybrid Cloud solution architecture service
(2) Creation of an on premise cloud transforming our traditional data centre services
(3) Creation of Hybrid Cloud services on top of public and private Cloud Infrastructures

10.1. Hybrid Cloud solution architecture

The deployment of a hybrid model requires DIGIT to provide guidance to the business and technical stakeholders in the European Commission to help foster sound decisions in a context where services offered are richer and more numerous but are also much more complex. Taking the right decisions in terms of architecture in such a context has an influence not only on the efficiency of an information system, but also on its security and its cost (for example, the cost of operations can vary by an order of magnitude, depending on the architecture).

DIGIT will support information system architects in making optimal choices with a solution architecture service that assists customers in the selection process of an operating model, hybrid hosting opportunities and with methodological (DevSecOps) and contractual choices, in line with its cloud broker role as described in section 5.4. By assisting and coaching information system architects to find the best cloud-native choices, it will assist the development community in closing the skills gap, as identified in the lessons learned, over time.

Technically speaking, DIGIT's solution architecture service will help DGs to identify which services are best suited for an information system, relying on services available in DIGIT's Hybrid Cloud service offerings. This support will be provided in the fields of:

- **Technical architecture:** DIGIT will provide support on technical and methodological choices. This includes the provision of validated and tested blueprints, patterns, guidelines, best practices and an architecture review service focused at improving security and reducing the cost of operation.
- **Data architecture:** DIGIT will provide support for data architecture choices to help ensure that architectures are "fit for purpose" and make optimal use of cloud data services.
- **Security and data protection:** As a detailed analysis in terms of security and data protection impact is mandatory. DIGIT will support DGs with the assessment of their deployment and operations with regards to IT security and data protection risks. GovSec, the common platform for cloud risk management described in section 5.2, will be the main vehicle to deliver this service.

10.2. Creation of an on premise cloud

The European Commission has a set of information systems that require the immunities and privileges protection of Article 343 of the TFEU. This excludes the usage of Cloud resources from Public Cloud providers who are not capable of providing such protection. These information systems will therefore need to run on premise in Data Centres of the European Commission for the foreseeable future.

However, the current operating model of our data centres cannot provide the same level of agility and security as a cloud-based operating model. In order to provide a similar degree of agility, control and transparency combined with an increased level of cyber-resilience of our on premise infrastructure, two challenges need to be addressed in our infrastructure: end-to-end automation and network segregation by design.

Addressing both challenges is precisely at the core of the ongoing "Private Cloud on Premise" programme. By automating our infrastructure processes end-to-end, this programme will allow information systems to benefit from the advantages of cloud computing also within the boundaries of our own Data Centres (e.g. self-service, increased speed of delivery, scalability, pay for use).

However, the “Private Cloud on Premise” program also addresses one of the historic weaknesses of the Commission’s IT infrastructure: insufficient network segregation. From the outside, the Commission network is well protected by firewalls. Once inside, however, IT resources have few restrictions to access each other. Although such a “hard shell, soft core” architecture simplifies the management of the IT infrastructure, this lack of segregation is reducing the Institution’s cyber resilience as, once inside, attackers can shift laterally without too many obstacles. A cloud-based operating model does not have this drawback. At the core of all cloud-native architectures is the notation of “segregation by default”: IT resources are placed in virtual “bubbles”, isolated from the rest of the world, with only well-defined connections explicitly allowed.

From this perspective, the transformation of our internal infrastructure into a private cloud on premise, will not only be an enabler for the EC’s digital strategy, but also a critical step forward for increasing the cybersecurity stance of the Institution.

However, DIGIT cannot compete with the broad market of cloud solutions available in the public cloud and replicate all imaginable cloud services on premise. It will therefore focus on a set of core services required by the information systems that need to run on premise, create new services that will be required to implement the European Commission’s Digital Strategy and provide the platform and services enabling new software delivery models like DevSecOps also for hybrid and on premise deployments.

In a first phase, DIGIT will create a number of services with a very low entry barrier to migration for existing information systems based on the most common architecture patterns (Weblogic application server with Oracle database backend), but with the properties of Cloud services (self-service, Infrastructure as code, segregation by default, …). This will facilitate the transformation of the application portfolio as described in section 5.3. Additional services to enable both lift-and-shift of existing information systems and the running of cloud-native information systems will be added over time.

10.3. Creation of Hybrid Cloud services on top of public and private Cloud Infrastructures

The consumption of public cloud services entails the management of a new set of technical service components and technologies. Lessons learned through Cloud1 highlight the complexity in setting up these services in line with service level requirements, notably underlining the significant shift in the so-called shared responsibility model. The conclusion is that DGs should profit of a corporate service layer, offering a seamless integration with Hybrid cloud services.

DIGIT will develop a homogenous service delivery layer with adherent service level commitments, leveraging capabilities available through the sourcing of services from the public cloud offering, while hiding the underlying complexities and warranting compliance with corporate rules.

The model will carefully address the challenge of balancing the need from DGs for additional support while permitting the consumption of innovative services made available through cloud providers. The service offering will consist of two parts:

(1) A core platform of foundation services for the secure consumption of cloud services, consisting primarily of networking, security services, identity management and data protection (at rest, in transit, in use). This is an inherent part of its role as Cloud broker for the European Commission, providing value-added cloud foundation services, as described in section 5.4.

(2) A set of strategic hosting services & technologies selected through product management and endorsed by corporate IT governance, responding to the bulk of service requirements and designed to meet the operational needs of critical information systems. This will enable the usage of cloud infrastructure while keeping the responsibility model currently provided by DIGIT, thus facilitating the cloud transformation for the system owners and reducing overall risk.

DIGIT will provide Hybrid Cloud services to the European Commission and interested institutions and agencies. To achieve this goal, it will create a Hybrid Cloud solution architecture service and transform the Data Centre to Hybrid Cloud services, built on top of both public and on premise private Cloud infrastructures.

11. DELIVERY OF CLOUD SECURITY SERVICES

The fact that European Commission cloud usage is still at an early stage offers us a unique opportunity to avoid legacy risks and implement an overall improved security posture for cloud ICT systems and services. This requires 'building-in security' at all stages of cloud deployment: from governance, risk assessment and management, procurement, the specification of common platforms and architectures, the management of hybrid cloud usage, interconnections between public and private cloud, administrative rights and access management, vulnerability management and patching protocols, specifying appropriate levels of log collection and storage and configuring security monitoring, detection and incident response.

DIGIT will supply a comprehensive set of Cloud security services to support information system owners on all hybrid Cloud flavours (private and public).

DIGIT will:

- Support System Owners to define and implement security controls and frameworks and provide ad-hoc security consulting services for cloud initiatives.
- Extend existing security monitoring and incident detection and response services to the hybrid cloud.
- Create a security service using pro-active threat hunting techniques to detect attackers that have already gained foothold inside networks of the European Commission.
- Support the DevSecOps processes with services like automated security assessments, vulnerability scanning, penetration testing and code audits.
- Run Red team exercises to identify and remediate weaknesses before these are exploited by adversaries.
- Create a security service that will pro-actively scan for "shadow IT" and accidental misconfigurations in the cloud.
- Support business and system owners with applying the secure system lifecycle and the EC risk assessment methodology and tools, in particular with regards to the use of GovSec, the common cloud risk management platform described in section 5.2.

DIGIT will provide cloud-enabled security services for all phases of the lifecycle of all types of consumption of Cloud services to the European Commission.

Annex I LESSONS LEARNED

1. CHANGED EXPECTATIONS DUE TO THE CONSUMERIZATION OF IT SERVICES

Consumers today have access to a wide range of cloud-based IT services for their private consumption. The ubiquity, speed of deployment and seamless integration of multiple devices that consumers experience with their personal IT devices is shaping their expectation for their workplace IT. Any perceived shortcoming of the workplace IT environment causes friction that leads to users augmenting or replacing workplace tools with personal, consumer-oriented Cloud services for their professional needs (i.e. “shadow IT”).

An example of such shadow IT is the corporate usage of the `dropbox` file sharing service. The absence of a corporate service that allows seamless sharing of files across multiple devices has led a significant number of European Commission users to create `dropbox` accounts with their European Commission mail address.

A second example has to do with the limitations around communication with staff outside the working environment. These limitations have led teams and groups to adopt `whatsapp` as a de facto communication tool. A DG has even based its BCP communication plan on `whatsapp`.

These examples of shadow IT highlight the ease with which corporate IT consumers can work around real or perceived shortcomings of their workplace IT environment. This creates obvious risks on the area of data confidentiality and especially reputation management.

2. OFF-PREMISE PRIVATE CLOUD PROVIDES LIMITED BENEFITS

When the Cloud1 framework contract was signed, it provided access to both public cloud and off-premise private cloud. One of the expectations was that off-premise private cloud would be the big initial growth area due to easy adoption. Instead, we found several surprising findings:

(1) The off-premise private cloud was a custom- and purpose-built environment just for the tender. In that sense, it was less of a cloud and more like managed hosting ("cloud washing").
(2) DIGIT found that, contrary to expectations, network integration between the private cloud provider and the European Commission internal network proved extremely complex and cumbersome.
(3) The only services offered by the Cloud provider were low-level infrastructure services. Any more advanced IT service would need to be built and managed by DIGIT.

Even though one agency was able to make successful use of the off-premise private cloud offer from Cloud1, the overall observation is that off-premise private cloud combines the worst properties of off-premise (the inviolability of the premise as guaranteed by Article 343 TFEU does not extend to such off-premise environments) and private cloud (limited service offering, limited scale, with increased costs) while offering no benefits when compared to the public cloud offering.

DIGIT and SG tried to benefit from cheaper storage in the private off-premise cloud and move the archive of Ares, the Hermes Preservation Services (HPS), to a storage service offered by the provider. But as this storage service failed to deliver the appropriate level of security (impossible to encrypt the data exchange between the European Commission premises and the storage service), this exploration was ultimately stopped.

3. SOURCING OF INNOVATIVE SERVICES

The global nature of cloud service providers (especially the hyper-scalers) allows them to react to market trends with unmatched agility. If they perceive a need for an IT service in a segment of the market, they can very quickly roll out generic multi-tenant services to all their customers.

An example of this is machine learning (a specific type of "Artificial Intelligence"). As demand for machine learning has taken off, many cloud providers have quickly started to offer specialised computing services for machine learning that are accelerated by the tremendous computing power of graphics processors (GPUs).

DGT was able to benefit from these services in the context of their eTranslation machine translation tool. eTranslation consists of two parts: the user visible translation tool and a backend system that continuously trains the translation engines. This backend system is an innovative machine-learning system that is a natural fit for cloud resources due to its "spiky" and unpredictable load pattern. DGT had already transformed its backend machine-learning system to a cloud-native system to benefit from the adaptive provisioning in the Cloud. When the cloud providers started to offer GPU accelerated machine learning services, DGT was able to immediately benefit from these services, significantly reducing the time and cost required to train translation engines.

4. BENEFITS OF ELASTICITY

The elasticity of the Cloud allows for quick adding and removing resources to information systems as needed. Cloud-native information systems use this elasticity of provisioning cloud resources to adapt their resource usage to their load. This creates two kinds of benefits:

- Reduced operational costs due to the metered nature of the cloud
- Better performance and reliability during unexpected peak usage

A prime example of such an adaptive IT system is the cloud-native new EUROPA platform. The number of visitors fluctuates wildly over the course of any given day, and launches of new European Commission activities can create even higher visitor activity. Due to the adaptive nature of the new EUROPA platform, IT resources are only provisioned when needed, resulting in a reduction of operational costs while providing a better experience at peak usage to users of the platform.

5. FULL BENEFITS OF THE CLOUD REQUIRE A TRANSFORMATION OF INFORMATION SYSTEMS

In order to benefit fully from the Cloud, applications need to be designed from the start for cloud platforms. Such cloud-native applications have modern application designs and use new ways of writing and maintaining these applications (like DevSecOps), which are more efficient than existing Enterprise-IT applications.

This does not mean that existing information systems cannot benefit from using cloud resources as well. Some existing information systems can be moved to cloud infrastructure ("lift and shift"), but even though they would then run in the Cloud, these information systems would not be able to fully benefit from cloud-native attributes such as elasticity and the cloud service marketplace. The real benefit of the Cloud for existing information systems comes only when transforming these information systems and their development teams to the design patterns and methodologies of the Cloud.

An example in this area is the experience of the Publications Office (OP) and their main publication platform EurLex. In the context of the Local Data Centre Consolidation program (LDC), OP triggered an ambitious migration project to quickly “lift and shift” EurLex and its supporting systems from the on premise data centre into the public cloud. The initial approach encountered several issues with legacy technologies at the core of EurLex that are not supported in the Cloud. OP has since retargeted the project to include a partial transformation of several parts of EurLex to facilitate the migration to the Cloud.

The European Maritime Safety Agency (EMSA) on the other hand decided to move several of their core information systems to the Cloud with a complete re-write based on a Cloud-native architecture. Using advanced Cloud Services as much as possible, EMSA managed to reduce the code base of these information systems by 95%. This radical improvement means that these information systems can be maintained with a reduced workforce and can be operated at a significantly reduced running cost. The drawback of the approach is the integral usage of vendor-specific advanced cloud services in the architecture, which increases the risk of lock-in with one particular cloud supplier.

6. THE CLOUD AS ENABLER OF A DATA-DRIVEN ORGANISATION

One of the most relevant factor for the success of the cloud is the ability to enable a modern way of managing (big) data. Data has become a critical asset of any organisation and needs to be exploited to deliver value. Cloud based data services and solutions to manage high volume of data and data operations are key elements for shaping the organisation of tomorrow.

The information system EUresults allows citizens to engage with the investments of the European Union in a meaningful matter. This was made possible through the construction of a data lake on top of cloud infrastructure, ingesting large quantities of structured and unstructured data, processing the data and creating a product that citizens can readily consume.

The European earth-observation programme Copernicus is running three Sentinel satellites and aggregates their high-resolution radar data on weather and land-mass changes. In order to facilitate public access to this massive data set, Copernicus created the cloud-based DIAS system of data access hubs. Together with five European Public Cloud providers, Big Data Infrastructures were created to store the raw data, allowing stakeholders to get on-demand access to compute power for exploiting the Copernicus data. This has created a data ecosystem that was simply inconceivable without Cloud.

7. IMPROVED OVERALL SECURITY POSTURE

Contrary to the belief that using public cloud resources would reduce the security posture of the European Commission, reality has proven that a correct usage of public cloud resources can actually increase the overall security resilience by removing internal risks.

Due to the need for administrator privileges, IT developer workstations present a significant security risk that is very difficult and therefore costly to mitigate. DIGIT created a “Service for Developers” (Srv4Devs) providing a service in the public cloud where developers can get a self-contained development workstation with testing resources in an isolated environment. This allows the European Commission to replace on premise developer workstations with cloud-based workstations that offer improved isolation. This solution provides better mitigation of the inherent risks of a developer workstation and removes security risks from its premises.

E-Mail is critical for the daily operations of the European Commission, but at the same time a constant source of risks due to e-mail based attacks ("phishing") that are difficult to distinguish from legitimate traffic. The European Commission has replaced its on premise e-mail filtering solution with a state-of-the-art public cloud-based business application. This new service is more efficient at detecting attack patterns and filtering them. The residual level of spam and phishing attacks dropped by 80%, significantly reducing the risks of cyber-attacks on the European Commission.

8. SECURITY MUST BE A PRIMARY CONCERN OVER THE LIFECYCLE OF AN INFORMATION SYSTEM

Modern multi-tiered information systems consist of a multitude of components that each potentially present vectors of attack for an attacker. Running these information systems in dynamically managed Cloud environments adds another level of complexity to an already complex system.

Several incidents have shown that securing information systems as an after-thought usually fails to address all possible security concerns. It is therefore necessary to have security as a primary concern during the lifecycle of an information systems. From completing a Business Impact Analysis before the design stage, to completing an IT Risk Assessment during the architecture phase to a DevSecOps process during development, implementing the right security measures at the right time significantly reduces the residuals risks for the information system Owner.

One such case resulted in not only significant financial impact on the Commission at the time of deployment, but also costs when trying to address the vulnerability while the application was "live".

9. INCREASED BUSINESS-CONTINUITY RESILIENCE THROUGH DIVERSIFIED SOURCING

The European Commission has built an extensive IT ecosystem that largely relies on IT systems running in the corporate Data Centres. These IT systems have developed many internal dependencies over the years and are tightly controlled from a few well-protected control points.

Cloud services from public clouds don't have the internal dependencies that traditional IT systems have. This diversification of sourcing and the implicit reduction of internal dependencies helps to improve the business-continuity posture of the European Commission.

The incident of 14.1.2018 (Skyfall) has shown that even with all the redundancy implemented in the Data Centre, there can still be hidden Single Points of Failure (SPOFs). A configuration mistake in an IT system management tool led to all windows servers in the corporate Data Centres being restarted at the same time. This led to a major and lengthy outage of all corporate IT tools, including all on premise corporate communication means (E-Mail, Skype for Business ...). During the resolution of the crisis, DIGIT crisis communication and coordination switched to the web-based conferencing solution (WACS). WACS is based on Cloud services in the public cloud which don't depend on internal services and was therefore not impacted by the Skyfall incident.

The Council has moved its alert system used to send SMS and e-mails to staff to the public cloud to be independent of their physical infrastructure in case of crisis.

10. SHIFT OF RESPONSIBILITIES TO INFORMATION SYSTEM OWNERS

Cloud computing offers a plethora of services to today's information system architects. Whereas in the past their choice was restricted to the services that corporate IT would make available to them, today there is barely a service that cannot be found on the market. But benefiting from this wide selection of services creates a dilemma for information system Owners.

With corporate IT, the boundaries of responsibility between the information system owner and the corporate service provider were static, clearly defined and well understood. This led to implicit assumptions on the split of roles and responsibilities. Now with Cloud computing, the roles and responsibilities might not be as clearly defined as in the past, or simply not well understood. This leads to the risk of a responsibility gap, where both information system architects and Cloud service provider assume that "the other" will cover certain responsibilities (e.g. patching of vulnerabilities). Additionally, implementing modern development methods like DevOps comes with a distinct shift of responsibilities between developers and operations, a trend which DevSecOps tries to mitigate by making security a core function of the development process.

With the experiments, DIGIT's broker function has clearly identified the responsibility gap as one of the most important and at the same time one of the hardest areas that need active management. Whereas the cloud broker can ensure a certain level of compliance via the procurement process, it is ultimately up to each individual information system owner to ensure that his information system has no responsibility gap, covering the residual risks.

11. SKILLS GAP

The first experiments that tried to use cloud resources very quickly learned that consuming IT services in the cloud was very different from running information systems in the corporate Data Centres. Even the best developers, system administrators and architects found that their existing skills do not translate easily to cloud environments. In addition, the Cloud has created a number of new roles that do not exist in traditional IT, but which are essential for the success of cloud projects. These roles include cloud architects, cloud engineers, cross-silo network, identity and security specialists, DevSecOps automation engineers and cloud migration consultants.

Some of those profiles can be found on the market today, but the competition for them is very strong. Unfortunately, external sourcing is not always a successful option. And for some information systems, the European Commission will probably decide that due to the sensitive nature of the position, some of these roles should be covered by officials.

All of these factors are showing that closing the skills gap will be a key success factor for the success of the transformation.

12. BETTER TOGETHER

The Cloud1 framework contract is open to all European Institutions and agencies. Having a common platform gave DIGIT in its role as inter-institutional Cloud Broker a better standing in the discussions and negotiations with the Cloud Providers and their assorted resellers. This in turn allowed the participating entities to benefit economies of scale that they would not have had on their own. Additionally, they can benefit from the continuity of service as the Broker service will continue to provide its services with a new framework contract.

13. NEW CHALLENGES IN RISK MANAGEMENT

The global marketplace of cloud-based business applications (Software as a Service) has triggered a shift of IT procurement decisions from IT departments to business units. Whereas previously big IT projects were required to deliver business functionality to end-users, the same functionality today is readily available in the Cloud with minimal initial configuration and establishment overhead.

This provides a challenge to existing corporate risk and security management processes which assume that the IT departments ensure and enforce the necessary links between the business units as system owners of information systems and their risk and security management counterparts. As business units these days are able to acquire cloud based business applications without the prior involvement of their IT department, this link is not established and corporate risk and security management processes are therefore working with an incomplete picture.

Governance of the procurement and operations of Cloud services needs to be further improved. The role of HR.DS as provider of the cloud outsourcing authorisation framework and of DIGIT as cloud broker and provider of the contractual framework is not fully understood across the European Commission.

14. PORTABILITY AND REUSABILITY

Cloud-native information systems are always architected and developed with a certain Cloud platform in mind. In order to reap maximum benefit from the chosen Cloud platform, the information system might be developed in ways that create difficulties for portability and reusability. This can lead to a vendor lock-in situation where data or information systems are tied to one particular vendor and can't be moved.

Such a situation is not inevitable though. The biggest risk is a situation where data cannot be moved to another provider, de-facto locking the whole information system to one provider. This can usually be avoided by careful design choices of the underlying data architecture.

A second concern is business functionality being implemented using services of a Cloud provider that due to the relative immaturity of the market and the absence of standards restrict the possible target platforms. This risk is greatly reduced when using cloud-native development methodologies, where "code refactoring" (rewriting parts of the code to improve maintainability and operability) is an essential tool in keeping the codebase modern, small and flexible. Changing from a service of one Cloud provider to another one should just be a refactoring cycle away.

15. THE INHERENT RISKS OF PUBLIC CLOUD DUE TO THE DISCREPANCIES OF EUROPEAN AND AMERICAN LEGISLATION CAN AND MUST BE MITIGATED WHEN DEALING WITH GLOBAL CLOUD PROVIDERS

All main public cloud suppliers operating in a global market, spanning multiple continents and dozens of countries. Such global economic operators cannot put the legislation of one country above the other. They have the duty to respect the law in all countries in which they operate, even if those laws are not always entirely compatible.

A recurrent question in discussion on the use of public cloud is whether the inherent discrepancies between European legislation (e.g. GDPR, our Privileges & Immunities) with the legislation in third countries (e.g. the CLOUD act in the case of the United States) is an obstacle to the adoption of public cloud.

In our experience with Cloud I, these inherent risks can be mitigated so that the resulting residual risk becomes acceptable. The mitigating measures are a combination of vendor due diligence, contractual provisions and technical security controls.

Although managing vendor risk is a key element of the cloud procurement process, it is not just a point in time but a continuous process. Managing vendor risk covers supplier specific policies (data residency, subcontractor risk, contract termination rights,…), but also the maturity of the service (attested through independent 3rd party audits), provisions with regards to the use of diagnostics data, etc…

The successful steps the Commission has taken towards Microsoft since 2017 with regards to the configuration of telemetry settings in its products, proves that such continuous vendor diligence can lead to positive results, not only benefiting the European Institutions but all European clients.

Contractual provisions are a second category of risk mitigation measures. They must provide clarity on Data ownership, Service Levels and how to handle Third-Party access requests (in the case of conflicting international legislation).

Technical security controls with regards to encryption, data loss prevention and digital rights management, together with on premise integration of logging and monitoring and Identity and Access Management facilities, form a third level of risk mitigation measures.

By combining such a broad set of mitigation measures, the inherent risks of public cloud can be balanced with the many advantages it offers, such as the increased level of cybersecurity resilience provided by the hyper scale cloud vendors.

However, as setting up such mitigation measures is clearly not trivial, the case for a central cloud broker providing a consistent baseline for all DGs and interested Institutions and agencies using public Cloud services becomes paramount.

Annex II GLOSSARY

Cloud Computing	Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.
Infrastructure as a Service	Infrastructure as a service (IaaS) is a standardized, highly automated offering in which computing resources owned by a service provider, complemented by storage and networking capabilities, are offered to customers on demand. Resources are scalable and elastic in near real time and metered by use. Self-service interfaces, including an API and a graphical user interface (GUI), are exposed directly to customers. Resources are usually multitenant.
Platform as a Service	A platform as a service (PaaS) offering, usually depicted in all-cloud diagrams between the SaaS layer above it and the IaaS layer below, is a broad collection of application infrastructure (middleware) services (including application platform, integration, business process management and database services).
Software as a Service	Software as a service (SaaS) are business applications that are owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics.
Cloud-native	Cloud-native is an approach to building and running information systems that exploit the advantages of the cloud computing delivery model. Cloud-native is about how information systems are created and deployed. It implies that the information system reuses existing cloud-based services, instead of relying on purpose-built data centre infrastructure services.
Hybrid Cloud computing	Hybrid cloud computing refers to policy-based and coordinated cloud service usage across a mixture of on premise and public cloud services.
DevOps	See DevSecOps
DevSecOps	DevSecOps represents a change in IT culture, focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach. DevSecOps emphasizes people (and culture), and seeks to improve collaboration between operations, development and security teams. DevSecOps implementations utilize automation tools that can leverage a programmable and dynamic infrastructure from a life cycle perspective.