EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

European Medicines Agency Cloud Strategy

Accelerating innovation and digitalisation for better public and animal health outcomes

Contents

Executive summary

EMA's newly developed cloud strategy takes into account both the increased adoption of cloud technologies at EMA as well as the evolution of the public cloud market in recent years. This strategy will act as a guideline for EMA's cloud adoption in the coming years, providing the Agency with the principles and approach to fully benefit from the potential of cloud-based technologies.

In 2017, EMA adopted a cloud strategy which promoted the opportunistic adoption of Software as a Service (SaaS) and "using public cloud solutions where the right controls can be put in place, where there is business value and where EMA can realise its business objectives". From a long-term perspective, the strategy endorsed "transitioning application and infrastructure platform services to a cloud-based provisioning mode".

This new strategy builds and expands upon this initial effort. It contains a built-in focus on security, data protection and compliance, which will be embedded in both existing and new solutions by design and can be elevated to new levels with the help of state-of-the-art solutions powered by the cloud.

It will accelerate digitalisation and innovation initiatives, increasing the return on IT investments and maximising the quality of EMA's services towards EU citizens and companies. More specifically, this strategy is aligned with the principles of the European Digital Strategy, and it will enable EMA to accelerate the adoption of the European Health Data Space, in particular the pillars regarding 'data quality and interoperability' and 'infrastructure and technology.

Adopting this strategy

will put EMA in a strong position to reach its objective of fully migrating to the cloud by 2025.

The opportunity

This new cloud strategy allows EMA to further transform its business and way of working in support of its mission towards public and animal health in the EU. Strategic adoption of the right cloud technologies will make it easier for EMA to meet its requirements regarding the exchange of data and collaboration at the European and global level. They enable a decentralised and collaborative method of exchanging large amounts of data in a secure and regulated way, without the burden of having to fully build and manage a large IT estate. By moving to the cloud, EMA will promote digitalisation throughout the Agency, allowing it to provide higher quality services to both its own

workforce and the public. The Agency will also benefit from capabilities which are only available in the cloud. The cloud offers access to modern and AI powered data lake solutions, built specifically for dealing with rapidly increasing amounts of data coming from a wide variety of sources. New insights and implications can be derived from unstructured data sources such as patient records and regulatory submissions.

Agility, speed & efficiency

The cloud will enable EMA to greatly increase its agility, speed and efficiency when experimenting and scaling new solutions.

Modern cloud platforms provide access to state-of-the-art technologies which were difficult or unrealistic to adopt in the past but can now be accessed and scaled at the click of a button.

They can be more efficiently incorporated into new solutions and updated or extended as new innovations hit the market, allowing EMA to efficiently respond to a rapidly increasing demand. Running both traditional and/or state-of-the art technologies is facilitated in the cloud as the cloud provides seamless updates and a very high level of availability and risk tolerance which would require substantial investments to achieve on-premise.

Additionally, new opportunities are becoming available for regulatory and administrative process automation and integration, drastically reducing the need for custom developed solutions which are difficult to maintain and tend to deprecate over time.

The cloud offers EMA an opportunity to adopt a more consistent approach towards technology in the future. Ad-hoc and custom solutions will be avoided whenever possible while still offering the flexibility and agility a modern public sector organisation requires to serve the ever-growing expectations of the citizens and businesses in the EU.

Considering EMA's experience with data centre procurement, increased cloud adoption will also guarantee improved stability in terms of the residency of EMA's solutions and avoid potential relocations of infrastructure driven by procurement cycles and other uncontrollable events. While relocations might still be necessary, relocations between cloud providers are less cumbersome than traditional on-premises relocations. Procurement cycles are still accommodated for in the context of a best-in-breed adoption of cloud technologies in a multi-cloud future.

The cloud also provides EMA with a high level of transparency with regards to what services are being used and which expenses they generate, making it easier for EMA to forecast, manage and report costs. Together with the various cost-saving payment models by the cloud, the cloud provides EMA with various options to be more cost efficient.

A modernisation mindset

Of course, realising these ambitions and benefiting from all the possibilities

offered by cloud is not a straightforward task. During its future cloud journey, EMA will carefully and consistently tackle the different challenges which are typical of such an engagement.

Compliance with security and data protection requirements and regulations

This is non-negotiable and will be implemented from the start in every step of the transformation and become part of a continuous improvement process for all operational environments.

Cloud comes in different flavours, mainly referred to as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service), with different levels of responsibility and flexibility split between the cloud service provider and EMA. The choice between these service models will be driven by user requirements, the stability or expected pace of evolution of the solution(s), and of course the familiarity of the EMA workforce with the technologies and their compliance with security and data protection requirements.

Besides selecting a service model to adopt, EMA will also establish an organisational and digital mindset oriented towards continuous learning and improvement. This strategy will link with other ongoing initiatives at EMA to influence a cultural shift towards this direction. This will help create a constant awareness and openness for modernisation potential in the application landscape of EMA. Through this strategy, EMA leadership commits to fostering such culture as well as prioritising initiatives and learning needs in order to ensure the capabilities of the Agency's IT teams. Processes and procedures for managing EMA's IT will be updated, and a solid cloud governance will be put in place to connect all relevant teams and help them achieve these goals.

EMA's IT teams are essential

Through them the Agency can accelerate the fulfilment of its ambitions by having access to the best possible solutions, they also have a key role in securing these environments and controlling the risks and threats to which an organisation is constantly exposed.

As the adoption and footprint of cloud technologies increases, EMA will constantly evaluate the skill requirements of its IT team and identify the gaps that might exist today, but also anticipate those skills which will be required in the future. To bridge these gaps, relevant training programmes will be developed and where relevant recruitment and sourcing strategies can be put in place to address specific skill gaps.

A trusted framework

A lot of bias and misconceptions still exist towards security and control when it comes to cloud. But when designed and used correctly, industry-leading levels of security, control and standardisation can be achieved which would be otherwise virtually unobtainable for most organisations. The intelligence and breadth of modern security solutions goes beyond the possibilities of what can be achieved at the level of an individual datacentre, while fully implemented governance and automation greatly reduce the risk of human error. EMA will leverage these possibilities in the cloud to ensure adequate security and protection of its information assets.

EMA will comply with relevant data protection regulations and rulings when moving to the cloud. More specifically, these include the Schrems II judgement and the Regulation 2018/1725 for EU institutions. In order to assess whether the legal and regulatory requirements are met, EMA will assess on a case-by-case basis whether a cloud project can adhere to these regulations and judgment and any future relevant laws, regulations and rulings.

Additionally, EMA shall take specific security principles into account when moving to the cloud, in order to ensure that the cloud is developed and managed in a way which is "secure-by-design". These principles act as guidelines in the design and/or adoption of cloud services, ensuring the security of the resulting solutions.

In order to act upon these requirements and deal with the shared responsibly of security in the cloud, EMA shall assign responsibilities related to security capabilities. These will be clearly defined in order to ensure that services are consumed securely and that security breaches are dealt with in an efficient and consistent manner.

In order to ensure that the appropriate governance tools are in place, thus allowing EMA to manage these responsibilities and ensure compliance with security requirements, four key domains on contracting, roles and responsibilities, policies and assessment are taken into consideration. These domains form an overview through which EMA will implement certain governance mechanisms in the cloud.

A trusted framework

Built upon a correct implementation of security and compliance solutions will allow EMA to transition to the cloud securely, responsibly and above all, compliant.

Of course, EMA is not alone in the definition of its trusted framework. It will be able to build upon earlier work performed by other EU Institutions and guidelines, in particular from the EDPS and EDPB. In the case of privacy, EMA will build on the work performed by the EDPS on investigating the Data Protection of Cloud Services such as Microsoft Azure and others.

Conclusion

This cloud strategy provides EMA with a trusted framework allowing cloud technologies to be an enabler and driver for digital business transformation and an agile operating model in the coming years. With this cloud strategy, EMA embraces the fact that cloud technologies will define the Agency's ability and speed to deal with the next generation of IT challenges to support new regulations and the needs of network the European Medicines Agencies Network. Cloud will give the Agency access to the tools and capabilities to expand its current services and accelerate its ability to deliver innovative services to European citizens and organisations.

1. Drivers and opportunities for Cloud Adoption

A successful cloud strategy operates under the principle that it equips EMA with a vision and decision-making framework that supports its mission, technology requirements and policy context. All of this starts with defining the drivers and opportunities for EMA to go to cloud, both from a business and a technology perspective as both dimensions are equally important to achieve the maximum potential of cloud adoption.

1.1. Drivers

The technological landscape is evolving at a rapid pace, driving EMA to adapt and evolve in order to meet new expectations and challenges. While not necessarily introducing new things to the organisation, drivers signify aspects to which organisations are forced to react if they want to continue their way of working in accordance with modern standards. Figure 1 provides a high-level overview of the different drivers for EMA's cloud strategy.

Improved information security

By moving to the cloud, EMA will start leveraging the cybersecurity capacities of the Cloud Service Provider(s) (CSPs). These companies continually invest billions in cybersecurity, ensuring they are compliant with the latest regulations and security standards. In other words, achieving this industry-leading level security would not be feasible for EMA through any other means.

Address rapidly increasing expectations regarding demand and interactions

As is the case for nearly all modern organisations, both public and private, EMA needs to respond to rapidly increasing demand stemming from a variety of sources, such as legislation, public health emergencies and emerging technologies and advances in science. By migrating to the cloud, EMA will obtain the agility required to address these needs, which has become increasingly difficult using the outdated custom-made IT delivery model.

The way that the public, stakeholders and the industry interact with each other is also changing drastically as the online/automated experience continues to gain importance. Switching to the cloud will allow EMA to adapt to these expectations.

Improved availability and resilience

By switching to the cloud, EMA will benefit from the availability Service Level Agreements (SLAs) made

Figure 1. Overview of EMA's drivers for moving to the cloud

IMPROVED INFORMATION SECURITY	ADDRESS RAPIDLY INCREASING EXPECTATIONS	SUBSCRIPTION BASED DATACENTRE	COST EFFICIENCY
EMA's cybersecurity level will be elevated to **industry-leading levels**	EMA will become **more agile and responsive to changes** coming from different sources	Challenges related to the obligation* of migrating EMA's **on-premises** infrastructure by March 2024 will be greatly reduced	EMA's will be able **to plan, manage and optimise costs** more easily, resulting in **substantial cost savings**

* as defined in the CANCOM-OC-EFSA-PTT-2015-01 framework contract

possible by the cloud, which are very costly to achieve on-premises.

Typically, the SLAs of major CSPs promise 99.X% uptime for their most basic services, which can be easily increased to >99.99+% for more advanced services.

Additionally, disaster recovery will be much easier in the cloud compared to on-premises, as cloud services can be restored from a backup in a much shorter timeframe than is usually the case for on-premises applications (seconds to hours, depending on the exact service and the selected type of disaster recovery).

Subscription based datacentre

Migrating to the cloud removes the need for relocations, significantly reducing the burden related to the relocation of on-premises infrastructure. This will enable EMA to have a more efficient usage of resources, both from a financial and a time investment perspective.

Cost efficiency

Switching to the cloud will assist EMA with increasing its cost efficiency compared to a traditional/non-cloud-based strategy. The main driving force behind this is the extremely high level of transparency that the cloud provides when it comes to costs. This is further explained in Section 5.

1.2. Opportunities

Next to the drivers discussed in the previous section, the cloud also opens the door to EMA to embrace a large variety of cutting-edge technologies, new use cases, more efficient ways of working and to reduce some pressing risks. These are highlighted in figure 2.

New capabilities for both IT and business

Switching to the cloud will enable EMA to start using completely new or heavily revamped capabilities, which will influence both IT and business aspects.

Examples of typical IT use cases enabled by the cloud are Artificial Intelligence, Machine Learning and Big Data. Adopting these new technologies will have a positive impact on business processes, as they provide new business insights and possibilities through a much more in-depth and efficient processing of data.

Getting started with these use cases in a normal scenario would require a massive upfront investment, but with the cloud EMA can simply leverage the investments made by the Cloud Service Providers.

Infrastructure Benefits: Improved SLAs

By moving to the cloud, EMA will be able to deploy infrastructure at an increased pace once the initial procurement has been completed. A comparison of the required time in the current situation and in a cloud-based situation is shown in figure 3.

Figure 2. EMA's Cloud Opportunities

NEW IT AND BUSINESS CAPABILITIES	INFRASTRUCTURE BENEFITS	REDUCE RISKS	MOVE TO THE CLOUD BY 2025	MODERNISE THE WAY OF WORKING
EMA will be able to **leverage cutting-edge technologies** (such as AI, Big Data), and **commodity services** (e.g. Email, Financial solutions).	EMA's infrastructure will become more **agile** and **available**, leading to **faster prototyping and higher resilience** against potential issues	EMA's risks related to both maintaining on-premises infrastructure as well as the datacentre migration are greatly reduced	This strategy will facilitate EMA's ambition to move to the cloud by 2025	EMA will adopt a way of working allowing for **easier cooperation** and **parallel working**

Figure 3. Infrastructure deployment requirements now and for the cloud

			Cloud estimation	
Tasks	**Time required Current situation**	**Actions Current situation**	**Time required**	**Actions**
Procurement of new hardware	2 to 6 months	**Approval** of the procurement Identify and negotiate with the **contractor** **Schedule** hardware delivery **Set-up** of the actual hardware.	None*	All hardware procurement is performed by the Cloud provider Multiple purchase orders no longer necessary as hardware provisioned on demand within contract limits (reduced procurement workload)
Deployment of new workloads/resources	2 days - 3 weeks	VM provisioning can be as fast as 2 days in **ideal case** Full **configuration** (firewall, vLANetc.) can extend the process	Minutes to days	**Automation** drastically cuts down on time Ideal case provisioning a VM only takes a **couple of minute**s Full configuration (firewall, vLAN etc.) can extend the process to a **couple of days**
Infrastructure maintenance and security vulnerability patching	1 day - 2 months	**Zero-day critical vulnerabilities** can be patched within a day, **resource-intensive activity** Usual patching **frequency of 2 months**	None to hours	Patch manager systems **automatically patch systems** as new patches become available Some manual patching may be required at times
Procurement of new software/tools	1 to 3 months	**Approval** of the procurement Identify and negotiate with the **contractor**	None*	Marketplace allows for rapid deployment of software

This makes it a lot of easier to test and prototype ideas, leading to overall faster experimentation. The scalability of any solutions leveraging this infrastructure is also drastically increased compared to solutions running on traditional hardware.

Modernise the way of working

Along with modernising the underlying infrastructure of the organisation, moving to the cloud also facilitates digital ways of working with improved collaboration and a stronger governance process. This will allow EMA to collaborate and communicate in real-time, to perform parallel reviews and co-author documents, instead of the traditional way of versioning and file check in/out.

Move to the cloud by 2025

This cloud strategy would allow for EMA to reach its target of fully migrating to the cloud by 2025.

Reduce risks related to maintaining large on-premises infrastructure

By moving to the cloud, EMA is relieved of the risks associated with maintaining on-premises infrastructure, including but not limited to:

- Security risks related to physical assets (fires, break-ins etc.). EMA currently maintains a lot of the burden of developing infrastructure security controls, and can simply not compete with the billion-dollar investments made by Cloud Service Providers;
- Risks related to providing adequate availability and business continuity. By relying on a single provider for data centre services, risks are elevated compared to the cloud model in which services are distributed between different data centres, potentially at a global level;
- Risks related to the ability of scaling up and supporting new workloads. This risk is the

counterpart of the 'Infrastructure Benefits' opportunity described in Section 2.2.

Reduce risks associated to the datacentre migration strategy

Currently, EMA needs to renew its datacentre contract every 5 years. Next to the contract renewal overhead, this activity also exposes EMA to a variety of financial and operational risks. This is further expanded upon in Section 5.

2. Cloud Migration Principles

When moving to the cloud, it is fundamental to lay out some key guidelines or principles which shall be adhered to during every step of the journey. This will ensure that EMA makes the correct decisions both at the start of and during the cloud migration, which can prevent various issues and wasted resources down the line. These principles shall be based on commonly accepted "best practices".

This section focuses on the different principles which will govern EMA's migration to the cloud. The services strategy, which lays out how different on-premises solutions/services should be moved to the cloud, is also included in this section as it dictates how the cloud migration will be executed.

2.1. Choosing the right migration strategy for each solution

Lift and Shift First, Optimise Later

While a "lift and shift" approach might be a good solution for certain cloud friendly application components which require few changes post-virtualisation, it is unlikely to be the optimal option for all applications (see the following section).

However, since EMA has to deal with contractual limits and overhead related to its datacentre, a "lift and shift first, optimise later" approach will have to be taken for certain applications which might not be a perfect fit for the approach.

This approach concerns a straightforward migration, where the current virtual machine (VM) size is matched to the closest instance type in the Cloud. This results in a fast, low-risk migration with easier compliance and security management in which the optimisation of the workloads occurs at a later point in time. The main objective of this approach is to meet a deadline or datacentre shutdown plan.

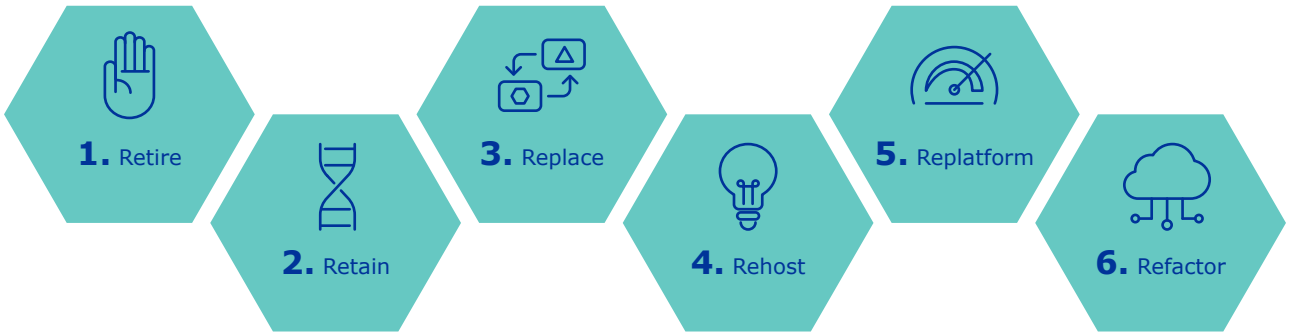
Even though a lot of the optimisation work is left for later, certain basic tasks such as sizing to peak utilisation, planning workload lifespans and running workloads safely under vCPU utilisation thresholds need to occur before the move to the cloud can be completed.

The 6 R's – A fitting approach for all types of application

When moving to the cloud, many organisations tend to either follow a "SaaS before PaaS before IaaS" strategy, especially when starting from the ground up. However, in the ever-evolving cloud landscape, the line between these three is becoming blurrier by the day.

A more nuanced approach will thus be taken, based on the requirements related to custom setups, regulation etc. For example, EMA will keep using SaaS solutions which are already in place, or switch to SaaS where solutions are readily available. For core/more specialised systems, on-premises solutions will be adapted to a IaaS model, and then

Figure 4. Path to Cloud: the 6 R's



gradually modernise by switching to PaaS for use cases where this makes sense.

While IaaS can be considered to provide 'direct' access to compute infrastructure, PaaS provides ready-made development and deployment environments that are managed by the CSP for users.

In order to facilitate this more nuanced approach, EMA will utilise "The 6 R's approach", depicted in figure 4. This approach defines the 6 main migration options to be considered during a cloud transformation. EMA will map each application/ component which needs to be migrated to the cloud to one of the 6 R's, highlighting the quickest path to a full cloud migration.

The mapping of all business applications can be integrated with the already existing "EMA Application Portfolio", where Application Lifecycle classification and Current / Target Delivery Approach have been already addressed.

This approach provides EMA with ways to deal with legacy/on-premises solutions which ensure that these do not become roadblocks and acts as an accelerator by providing a tried-and-tested approach for almost all potential migration use cases.

A short description, as well as an example of a good fit for each approach is given below:

- **Retire:** For applications that are to be retired / end of life, possibly with users migrating to another application. This could be a good option for custom .NET or Java applications with features that can be consolidated in an OOTB or ERP package;
- **Retain:** Leave the application as a part of the on-premises legacy infrastructure. This solution would be a final resort for business-critical legacy applications which cannot be moved to the cloud;
- **Replace:** For applications that are to be replaced by another application (or set of applications) and use commercial software which is delivered as a service. This is a suitable method for commercial off the shelf (COTS) platforms which are currently not deployed as SaaS but can be replaced by a SaaS alternative. Virtually all the major software vendors used by EMA provide SaaS alternatives for their software. This approach is best suited to SaaS.
- **Rehost**: For cloud friendly application components which require few changes post virtualisation. This is a lift and shift of the application onto a Cloud IaaS stack or a container (CaaS). This approach can be applied to any Windows or Linux virtual servers with cloud friendly workloads (i.e. small application footprint / minimal dependencies & interfaces and configuration changes on OS, Webserver, Approver, DB Stack level only- instead of at the application code level). This approach is bested suited to IaaS (and CaaS).
- **Replatform:** For application components which are not available or cost-effective in the cloud and therefore need to be adjusted. This would be necessary for workloads where an OS/software upgrade or shift in database packages would be required in order to run in the cloud. This approach is best suited for IaaS and PaaS, the choice between the two depending on the availability of relevant platforms.
- **Refactor:** For applications which are not compatible with the cloud or where business

Figure 5. 6 R's Migration Paths

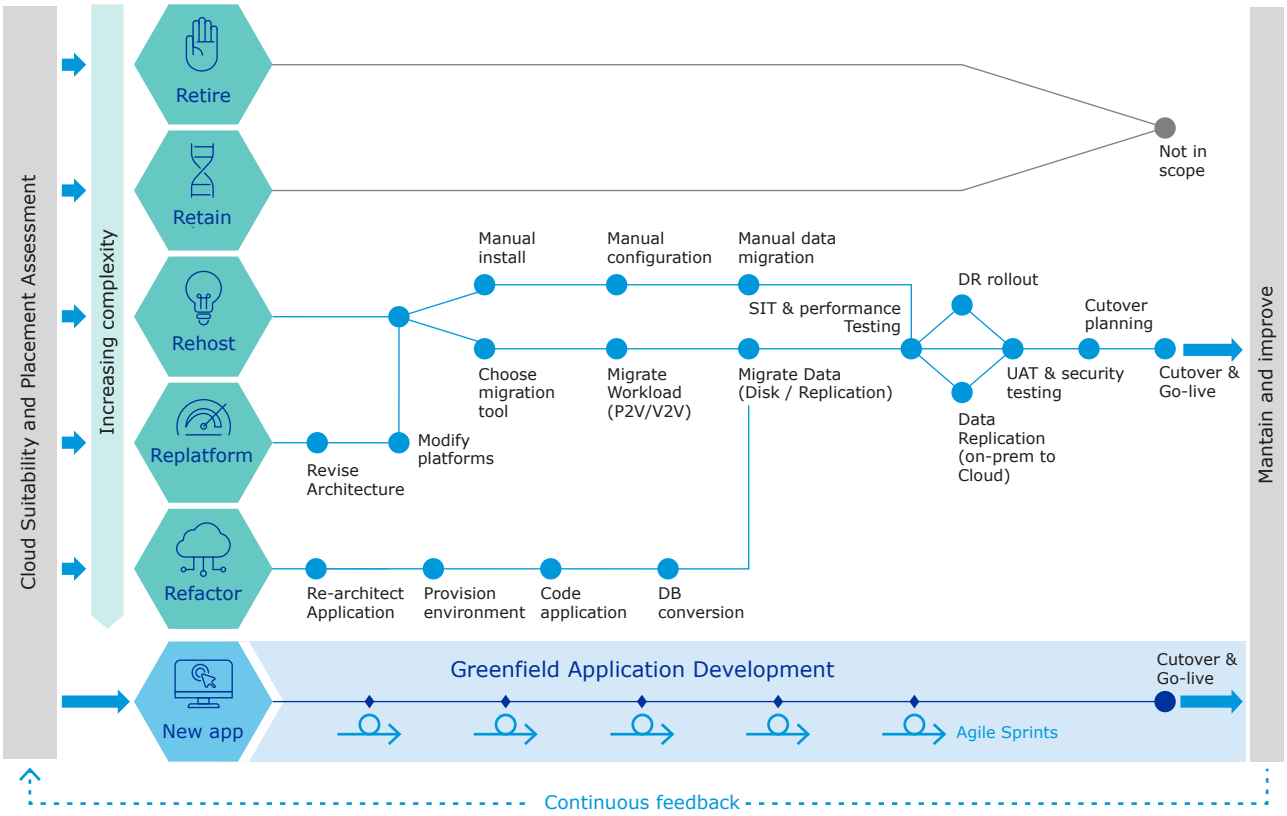
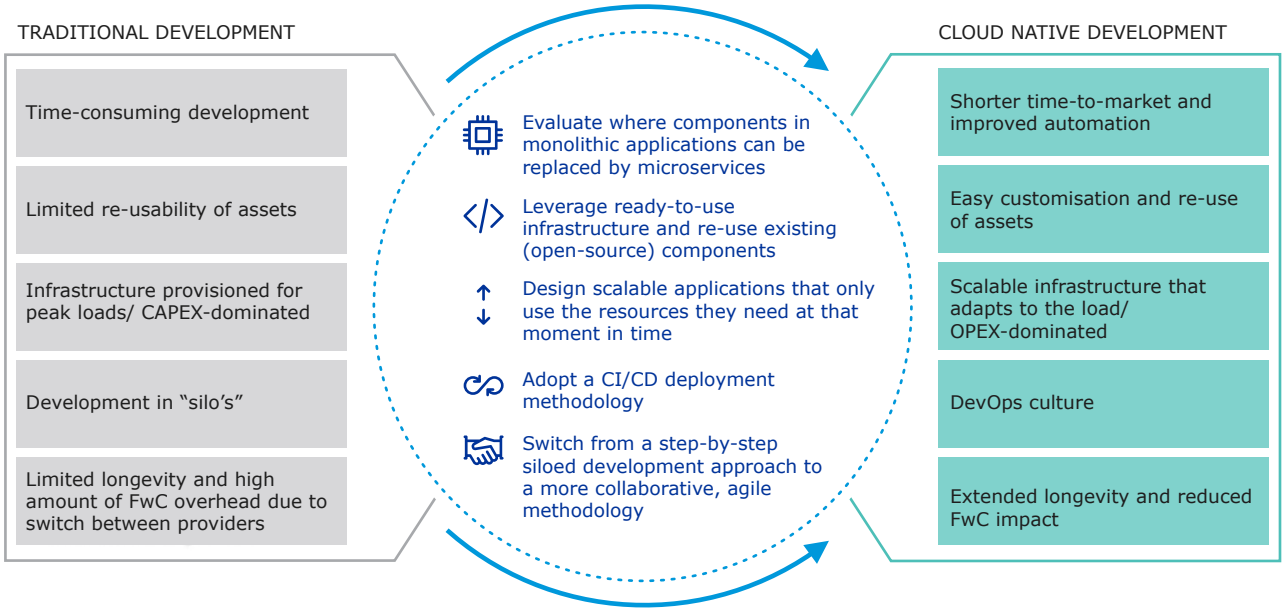


Figure 6. Transition to Cloud Native: from traditional to cloud native deployment



requirements demand that the application becomes more cloud native. Monolithic/non-RESTful applications might need to be refactored to fit in with the cloud. This approach is best suited to a combination of IaaS, CaaS, PaaS and FaaS, depending on the specific layer of the application which will be refactored.

Once all applications and components have been mapped, a relatively consistent approach can be followed for each component depending on which "R" they have been mapped to, as depicted in figure 5.

While this section laid out the different possible approaches which will be leveraged by EMA to migrate to the cloud, it has not yet touched upon what should be considered the ultimate end-goal of a cloud migration: a cloud native organisation running cloud native applications.

Cloud Native

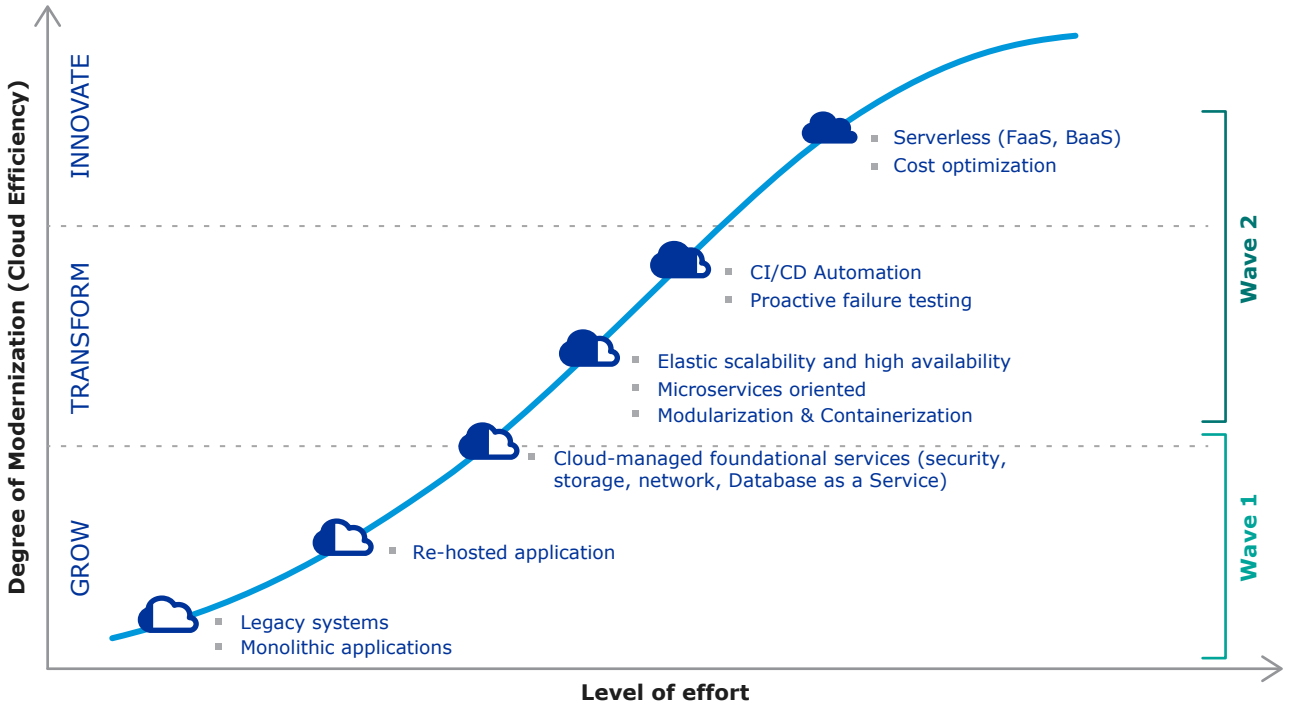
The Cloud Native approach to developing and Cloud Native applications are the perfect example of how working in the cloud should be done, although adopting this approach in all aspects of an organisation such as EMA is a resource and time-intensive task.

Shifting to Cloud Native development/ technologies will empower EMA to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

These techniques will make it possible for EMA to drastically reduce the time-to-market of their application by leveraging automation, easy customisation and by reusing assets. Cloud native solutions are by default powered by scalable infrastructure which can easily adapt to variations in the application load. DevOps is also a staple of Cloud Native development, which reduces the "siloed" way of working prevalent in most organisations.

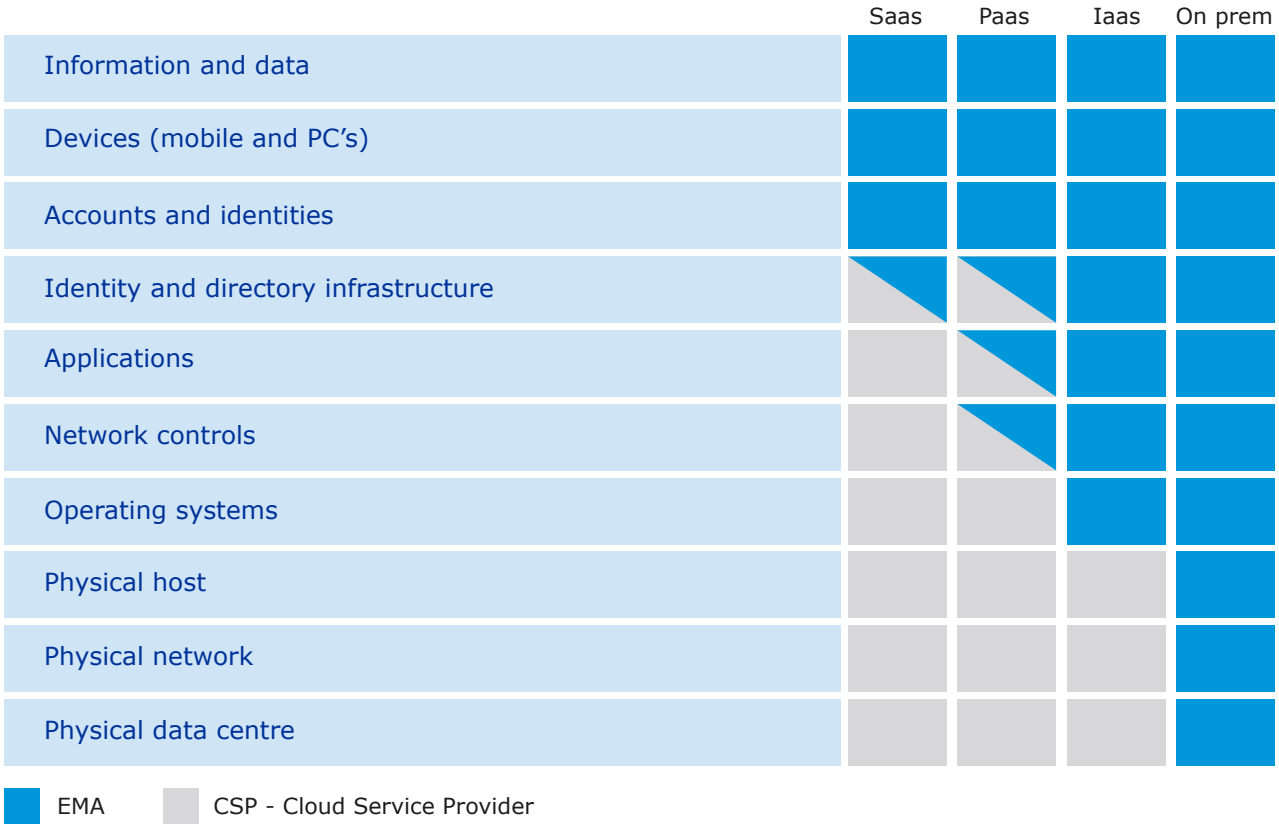
Figure 6 highlights the steps that will be taken to switch from traditional development to Cloud Native development, as well as the impact of this transition.The Cloud Journey

Figure 7. EMA Surveys to companies with PRIME products



Wave 1: Quick-wins typically addressedduring migration **Wave 2:** Full value of Cloud

Figure 8. Responsibilities of EMA vs. Cloud Service Provider



The Cloud Journey

When talking about migrating to the cloud and the cloud native way of working, it is important to raise the point that the cloud is not an all-or-nothing proposition. Rather, moving to the cloud should occur according to a phased approach, as depicted in the figure below.

The migration to the cloud and cloud native will be evaluated for different applications/components in accordance with the '6 R's approach', also considering the requirements related to costs, timing and knowledge as well as the potential for standardisation and portability.

Switching all applications to a cloud-native approach is thus not necessarily the best solution for EMA. Only by making a balanced decision between these factors will the correct choices be made when it comes to transitioning to the cloud and the cloud native approach of working.

2.2. Consider which responsibilities should be taken on by EMA

One of the most important factors to consider when migrating an application to the cloud and deciding on how to approach this (IaaS, PaaS or SaaS) is the responsibilities associated with each type of service. As is visible in figure 5, the responsibilities differ drastically for the different service types as shown in figure 3-5 above. A decision will be made about which responsibilities should and can be handed off to the Cloud Service Provider for each service, based both on the regulations/guidelines which govern EMA, as well as the expertise currently available within EMA.

2.3. Buy before Build

When a new need arises, it is always a good idea to verify if a solution which addresses this need can be bought instead of building it from scratch. This will improve the cost efficiency while reducing the complexity and time-to-market, and these

solutions will also adhere to market standards and best practices.

Furthermore, risks associated with the deployment and maintenance of a new component are evaded, and the requirements related to workforce experience/expertise are a lot lower. One additional point to considered here is to limit the customisation of packages in order to avoid high costs related to upgrades and patches, which become more complex as customisation increases.

2.4. Multicloud

One of the major principles which will be taken into account during EMA's cloud journey is that of Multicloud, which simply means that EMA will not choose one single CSP and its solutions as their 'default' way of working, but rather evaluate different CSPs and their solutions for each scenario and select the best fit.

Next to being a commonly accepted best practice, the European Commission published its Cloud Strategy in 2019 which encourages Multicloud based on the following two reasons:

- It prevents the EC from being tied to one public cloud provider (i.e. lock-in);
- It allows for sourcing the cloud provider best suited to the requested service.

EMA will adhere to this principle and leverage Cloud Service Providers including the ones in DIGIT's Cloud II Framework.

2.5. Monitoring of KPIs related to the execution of the strategy

In order to ensure that the execution of the strategy proceeds smoothly, EMA will monitor key performance indicators (KPIs) related to the drivers listed in Section 2.1. Examples of such KPIs are listed in the table below.

Figure 9. KPIs for the execution of the strategy

KPI	Definition	Measurement formula
Cloud Roadmap Delivery	Monitors cloud roadmap activities completed on time	# of priorities that are completed on time
Application Cloud Suitability	Measures applications analysed for cloud suitability assessment	# of applications analysed for cloud under each migration path
Application Total Cost of Ownership (TCO)	Monitors and analyses app TCO reduction after cloud migration	Reduction in costs due to cloud migration
Business Case Development	Monitors and analyses the reviewed business case	# of approved and completed business cases
Automation Maturity	Measures different aspects related to the automation of various cloud processes	% of provisioning speed increase, # of auto-remediated non-compliant services and environments, # of services automated / in progress / planned etc.
Security risk mitigation	Monitors the number of detected and mitigated security risks on Cloud	# of identified and resolved security issues on Cloud
Governance Compliance	Monitors compliance of governance and security policies	% of compliance with security policies
Server Downtime	Measures the server downtime in minutes, both planned as well as unplanned downtime	Server downtime in minutes due to planned or unplanned events / incidents
Time to Spin Up New Environments	Measures average reduction in minimum time to spin new environments	Average reduction in time to spin new environments

2.6. Further guiding principles

EMA will consider some additional guiding principles when looking at provisioning services:

- EMA will take user needs into account when deciding between IaaS, PaaS and SaaS. For example, if routing flow or data entry options are important, IaaS will be prioritised over SaaS, as IaaS provides more customisability compared to SaaS;
- The customisation of applications will be limited to go no further than simply addressing a/ multiple business need(s). The more "generic" an application is, the easier it is to troubleshoot or migrate to other environments. Furthermore, continuous development is also easier for less customised applications, as bespoke functionalities tend to break more easily;
- Applications will only include 'cutting-edge' components when these bring an actual value. Adding these components without a specific reason introduces unnecessary complexity into the environment, which increases the risk of failure;
- EMA will prioritise commercially available solutions when possible, instead of building their own application from scratch.

3. Financial Consideration

3.1. Cost Transparency

All the major Cloud Service Providers provide a variety of tools which allow their users to forecast, manage, report and optimise the costs incurred in the cloud.

Forecasting/Planning

Before moving to the cloud, CSPs provide easy-to-use solutions to help estimate the total cost (savings) associated with moving to the Cloud. This can be done manually, or with the support of the Cloud Service Providers themselves, as was done by AWS for EMA in the previous subsection.

Managing and reporting

Once the transition to cloud has been completed, allocating costs to a specific project/service/ department can easily be accomplished through a variety of methods (e.g. department specific accounts, grouping, tags etc.).

In addition, the cloud provides near real-time visibility of costs and usage information and provides various tools to visualise and analyse this data.

This makes it straightforward for management/ leaders to track usage, manage billing and control costs incurred in the cloud, which will allow for easier balancing of the (IT) budget.

EMA will define internal processes which will govern the approach for cloud financials. It will also set clear rules and establish guardrails which it will use in order to enforce compliance with this approach.

Optimising

The cloud allows its users to continuously optimise their spending based on their current needs. Some CSPs even provide you with their own recommendations to ensure cost optimisation, both from a resource as well as from a payment model perspective.

3.2. Payment models

Financing workloads in the cloud follows a different approach from on-premises infrastructure. Instead of incurring a large CAPEX cost at the beginning of the lifecycle of the infrastructure, as is the case for on-premises infrastructure, the cloud offers a pay-as-you-go approach.

With this approach, you only pay for services for as long as you use them, without requiring complex licensing or long-term contracts. In other words, the infrastructure (and its associated cost) used by the organisation can scale dynamically with the workload. This reduces the need to take depreciation into account when reviewing an organisation's financials.

The benefits of pay-as-you-go model can be further enhanced by:

- Committing to using infrastructure for a set amount of time (usually 1-3 years). By "reserving" infrastructure for a certain period in advance, the total cost will be lower than if this infrastructure would be provisioned for the same period according to the pay-as-you-go model.
- Using more cloud services. The price per unit of cloud services tends to decrease as the total volume used goes up.

4. Data protection and security

This chapter describes the Security component of the overall cloud strategy.

4.1. Data Protection

Compliance

For the privacy and data protection regulatory expectations, this document builds upon the earlier established Data Protection and Information Security Requirements policy (27-07-2016) from EMA. This document already outlines data protection and security requirements for third party hosting, including cloud services. For the purpose of this document, several privacy and data protection requirements are defined in addition to the original document to account for changes in privacy and data protection requirements since the creation of the requirements.

The importance of this section is underlined by the EDPS Order of 2020 pursuant to Article 58(1)(a) of Regulation (EU) 2018/1725, in which the EDPS[1] 2urges EU Institutions to take a precautionary approach to contracting U.S. service providers (e.g. public cloud) and establishing new processing operations with these services providers. This order follows in light of the Schrems II judgment and the subsequent privacy risks for personal data transfers outside of the EEA. Hence, this chapter will outline the precautionary approach taken by EMA for the processing of personal data. Essentially this entails a case-by-case approach which will assess what personal data under which conditions might be processed by a cloud service provider within and outside of the EEA.

EMA's roadmap to cloud

The overall goal of this chapter is to describe what EMA will do to go to the cloud while remaining compliant with relevant data protection

EMA's approach to data protection shall be risk-based. In order to realise this, EMA will inventory personal data affected by the use of a system/ application and assess for each of these applications/systems the possible risk(s) for data subjects in a cloud context. Accordingly, EMA will manage this risk and mitigate or avoid these risks based on the impact of the risk posed for data subjects and the applicable rules in Regulation (EU) 2018/1725. As to possible international transfers in the absence of an adequacy decision by the European Commission for the relevant country, careful consideration shall be given to the need of introducing supplementary safeguards in addition to those provided in Chapter V of Regulation (EU) 2018/1725.

Personal data refers to any information relating to an identified or identifiable natural person (the data subject). In the EMA context this includes, but is not limited to, medical data, administrative and

1 Guidelines on the use of cloud computing services by the European institutions and bodies, EDPS, 2018, https://edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

financial information about an individual. Storing and processing this data in the Cloud requires a data controller (EMA) to consider protection and security of this data and compliance with data protection law by its data processors (Cloud Service Providers, in this case).

To address the above, this chapter describes the following sections:

- Key aspects that will be addressed
- Compliance with regulations

Key aspects for Data Protection and Security

This section describes key data protection aspects for data controllers during adoption of Cloud services for processing of data:

- **Data quality and accuracy:** Well-organised datasets prevent mishandling or unexpected exposure of data. In addition, EMA ensures that incorrect personal data is not processed.
- **Data minimisation and purpose limitation:** The purpose for which personal data is processed will be registered and will ensure that no more personal data than necessary will be processed. For processing and transfers the purpose of data operations will be registered at the moment of data collection and that additional processing activities need to be validated with the original purpose if there is a need for additional use of data.
- **Right of information:** This right enables data subjects to be informed about their rights and for what purposes their (health-related) personal data is processed. Managed alerting and notification services provided by cloud service providers will enable EMA to automatically inform data subjects in a timely fashion, thereby reducing substantial operational overhead.
- **Right of access:** The availability feature of cloud services makes them conveniently accessible to end users. On the other hand, it will also allow possibilities for EMA to automate this process. Moreover, data portability will be ensured.
- **Data retention:** Personal data may not be stored longer than needed for the predefined purpose. Therefore, retention periods will be implemented, and data will be effectively deleted across all data storages when retention periods expire. To identify and manage multi-jurisdictional retention requirements, we will implement the following best practices:
  - Contractually stipulate the retention and deletion policy that must be implemented;
  - Stipulate contractually that the Cloud Service Provider will support EMA with deletion of data in all locations if required;
  - Different jurisdictions may have different retention rules for personal data; hence, these jurisdictions will be identified.
- **Privacy-enhancing technologies (PETs):** Privacy-enhancing technologies ensure the safeguarding of data protection principles. EMA will consider which PETs add value to the cloud strategy. Best practice is, for example, the encryption of data storage with customer-managed keys. Hence, EMA will focus on embedding PETs in the adoption of the public cloud.
- **Data security:** Personal data needs to be adequately protected. Hence, EMA will utilise the existing risks management practices and define further technical and organisational measures for cloud usage to ensure data is adequately protected and take up their part of the shared responsibility in cloud management. Conversely, EMA will ensure Cloud Service Providers also manage their part of the shared responsibly in adequately implementing data security practices.
- **Access to data:** Best practice is to limit access to data to people from the organisation on a need-to-know basis. However, it could be the case a CSP wants to access the environment. This type of access by the provider shall be managed on a case-by-case basis to ensure compliance with relevant rules and regulations.
- **Procurement of Cloud Services:** Before procurement of cloud services/providers there needs to be a (privacy) risk assessment performed that assesses whether the envisioned data operations may be performed, privacy risks can be managed, and the providers offers a sufficient level of security measures. This risk assessment may be performed in line with existing EMA risk management practices. The outcome of the risk assessment will be used to further enhance SLA requirements and/or

contractual clauses if necessary. This will be done according to the guidelines defined by the EDPS11. In addition, earlier recommendations from the EDPS' investigation of Microsoft services that include recommendations for EU institutions will also be implemented. These recommendations are as follows:

- Ensuring proper contractual safeguards in place for data transfers, data location requirements and transparency on data disclosure requests;
- Ensure sufficient purpose limitation of data processing by third-party providers and/or implementing adequate measures to mitigate insufficient purpose limitation;
- Ensure an adequate data processing agreement is in place with third-party processors;
- Define an overview of sub-processors of a third-party provider, whenever possible;
- Contractually stipulate that use of sub-processors can only be implemented after explicit permission of EMA as a controller;
- Perform a DPIA on cloud services/products before adoption.

Given the sensitivity of personal data processed by EMA, additional measures will be taken to ensure CIA (Confidentiality, Integrity and Availability) of this data. This will be achieved by establishing stringent policies and technical guardrails for data protection and security.

Compliance with regulations associated with Data Protection and Security in Cloud

Regarding data protection regulation and rulings there are two specific authorities against which compliance will be assessed and managed: Regulation (EU) 2018/1725 and Schrems II.

According to Article 4 of Regulation (EU) 2018/1725, data quality refers to a set of main principles which can be realised in a well architected cloud environment.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Regulation (EU) 2018/1725

Regulation (EU) 2018/1725 recognises data protection (of personal data) requirements for EU institutions like those defined in the General Data Protection Regulation. Thus, protection of this data in cloud environment is of utmost importance.

Schrems II

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling regarding the transfer of personal data of European individuals outside the European Economic Area (EEA) (Schrems II). In the judgement, the CJEU has confirmed that data exports to third countries that cannot guarantee the same level of protection to EU residents that the EU provides are not allowed. In addition, the CJEU ruled that the EU-US Privacy Shield was no longer a valid mechanism to transfer personal data from the EEA to the US.

These principles will be realised while designing the architecture for the cloud environment which will process personal data, in order to ensure and demonstrate compliance with this regulation. To fulfil these principles EMA will utilize guidelines provided by the EDPS to adhere to these requirements in a context that considers the different services models of the cloud such as SaaS, PaaS and IaaS.

As a result of this ruling, EMA will also ensure that the cloud strategy appropriately addresses concerns raised by the CJEU. In addition, EMA will also take into account the EDPB[3] recommendations on public-to-public transfers that are relevant to

3 Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, EDPB, 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

EMA as a public institution.

EMA will consider the following recommendation as given by the European Data Protection Board:

*As a data controller, EMA will ensure that access shall be restricted for the public authorities of a third country to which the data is exported if that country does not offer effective (i.e., EU standard) remedies for individuals against that acces*s.

Accordingly, EMA will consider on a case-by-case basis the following requirements for each cloud business case based upon the recommendations as given by the European Data Protection Board and the European Data Protection Supervisor. The following recommendations are also aligned to the original Schrems II judgement. In addition, EMA will aim to align with existing guidelines from the EDPB on cloud computing usage between public sector organisations outside of the EEA.

Know

- Transfers:
  - EMA will ensure awareness of where personal data goes, including remote access from third countries, and storage in a cloud outside the EEA;
  - EMA will verify that data that is transferred is adequate, relevant and limited to what is necessary for the purpose for which it is transferred ('data minimisation').
- Transfer tools:
  - EMA will identify the transfer tool which transfers utilise. This will be performed to ensure that the transferred personal data has an equivalent level of protection as the EU;
  - For occasional transfers, verify that all conditions for Article 50 from Regulation (EU) 2018/1725 are met;
  - EMA will also monitor for changes in transfers.

Assess

- Third countries:
  - EMA will assess and consult the data importer where necessary to determine the level of protection in the third country data is transferred to;
  - EMA will consider the circumstances of the transfers (e.g., categories of personal data);
  - The focus shall be on relevant law and objective factors that may require importers to disclose personal data to public authorities.
- Supplementary measures:
  - EMA may have to identify and adopt supplementary measures (e.g., encryption, pseudo anonymisation, splitting personal data), on a case-by-case basis;
  - Contractual, organisational and technical measures will be implemented;
  - EMA will avoid, suspend or terminate the transfer if no supplementary measures are suitable;
  - EMA will consult the supervisory authority where necessary.

Monitor:

- Data importers:
  - EMA will have mechanisms in place to ensure that transfers are suspended or ended if data importers breach their commitments.
- Map of destinations:
  - EMA will have a mechanism in place to ensure that transfers are suspended or ended if supplementary measures are no longer effective in a third country.

Requisites for risk-based approach to data protection

Accordingly, in order to decide what processing/ transfers may occur EMA must decide on what personal data of data subjects cannot leave the EEA due to significant privacy risks. On the other hand, this also entails that EMA will decide on what personal data may be migrated to the cloud given that it can be protected adequately by incorporating adequate security measures by design.

In the case that EMA does consider proceeding with non-EEA and possible inadequate third-country transfers then it will follow the EDPB guidelines on

proceeding with these types of transfers. Specifically, in this case EMA will need to demonstrate and document via assessment, in collaboration with the data importer, that any problematic third-country legislation does not pose a threat to transferred data while taking into account experiences of other organisations, provided that - in addition to adequate security measures being taken, as described below - appropriate supplementary EEA-type safeguards are agreed upon with the data importer for the purpose of compliance with obligations set under Article 46 of the GDPR.

Measures to be implemented in the case of a non-EEA personal data transfer

In the case of a personal data transfer outside of the EEA the EDPB recommends three types of the supplementary measures that may be implemented to provide effective EU-level data protection safeguards. It is important to note that the effectiveness of the implementation supplementary measures must be assessed on a case-by-case basis. Moreover, the measures listed below are not exhaustive but indicative of the measures EMA will consider per case to ensure the adequate safeguards are in place to protect data by design. The EDPB recommends the following types of measures:

Technical measures

- The EDPB considers encryption an appropriate supplementary measure if:
  - It is state-of-the art, considering not only technological design, but also the third-country authorities' capabilities and resources against such encryption;
  - The encryption algorithm is flawlessly implemented, encryption keys are reliably managed, and control over the keys is held by the data exporter located in an EU country or a country with adequate level of protection. If data is transferred to a protected recipient, control over decryption keys could also be held by the recipient;
  - Back-door access is ruled out. Whereas a backdoor constitutes an unauthorised access mechanism.
- The EDPB considers pseudonymisation an appropriate supplementary measure if:
  - It is not possible to identify a data subject with any additional information that the third-country authorities may hold, or obtain via other channels;
  - Additional information is held only by the data exporter located in the EU or a country with adequate level of protection;
  - Technical and organisational measures are in place to prevent disclosure or unauthorised use of additional information.
- The EDPB considers splitting personal data an appropriate supplementary measure if:
  - (Sub-)processors that receive the split data are located in different jurisdictions;
  - There is no evidence of collaboration between the authorities of the different jurisdictions;
  - It is not possible to identify a data subject with any additional information that the third-country authorities may hold or obtain via other channels.

Contractual measures

Contractual measures themselves may be useful for third countries with already similar EU-level remedies for data protection. As a third-country government is not bound to contractual clauses between organizations this might only help if the aforementioned conditions are met;

The following measures may support the safeguarding of personal data:

- Ensuring the contractual obligation to use specific technical measures mentioned above;
- Ensure the power of the data exporter to enforce audits, only effective if:
  - Access and audit logs are tamper proof to see evidence of access;
  - The scope covers the relevant processes and systems.
- Contractually require the data importer to report if a third country is no longer able to offer EU-level equivalent data protection, but only effective if:

- Notification is given before access;
- The importer monitors data policy developments;
- Data portability/data restriction measures are in place for the exporter.

Organisational measures

Organisational measures that may support contractual and technical measures are:

- Internal polices outlining for example the mandatory assessment of third countries and the assessment of supplementary measures for potential data transfers/data processing;
- Security standards for controllers and processors that third parties should at least utilise to ensure that is protected consistent with some form of standard (e.g., audits for third parties).

4.2. Security Compliance Requirements

The ISF recognises three main challenges with securely moving and managing the (public) cloud:

- Identifying and maintaining the appropriate security controls;
- Balancing the shared responsibility for security between the CSP and cloud customer;
- Meeting regulatory requirements to protect sensitive data in the cloud environment.

The goal of this security strategy is to firstly acknowledge these challenges posed to the overall information security of EMA. Secondly, this security strategy defines three guiding policies to manage these challenges.

The guiding policies, or in other words solutions to the challenges are as follows:

1. Defining Cloud Security principles

What design consideration does EMA need to adhere to when adopting and maintaining the cloud.

2. Defining a shared responsibility model

What does EMA need to define in order to manage the complexity of the shared responsibility model and consequently shared security controls in a multi-cloud environment.

3. Defining a cloud security governance model

What governance model for security does EMA need to adopt and what design considerations need to be taken into account when adopting and maintaining the cloud.

State security principles

In order to guide the secure adoption and management of public cloud services, we identified a selection of security capabilities which will be managed when moving workloads to the cloud. For these security capabilities, specific guiding principles are defined.

Security principles:

Adoption of Cloud Services

- **P1 – Assessment of CSP and Cloud services**. Description: Before the adoption of cloud services and new service providers. EMA will consider the review of contracts, third-party reports of compliance, available audits and certifications of cloud providers. This review serves the purpose of identifying any gaps in security requirements. Finally, it is important to analyse the impact of unprompted changes in services and contracting from cloud service providers and relating them again to the gaps in security requirements. In addition, proper incident management in case of a breach will be in place.
- **P2 – Secure Cloud Consumption**. Description: Understand the security requirements of the cloud services offered and what would be a safe service configuration. EMA will determine the allow-list of cloud services offered by IT and ensure these services are vetted. In the case of unvetted cloud services, educate staff on security and perform periodic security reviews.

Identity and Access management

- **P3 - Identity as the perimeter**. Description: In any case treat identity as the main perimeter instead of delineating the network as the perimeter in the cloud. Furthermore, this also entails centralising the perimeter due to the multi-cloud content. Hence, a centralised IAM

and/or CASB solution will be used in the multi-cloud environment.

- **P4 – Least privilege in the Cloud**. Description: To prevent a lack of fine-grained roles and access in the cloud, a process will be defined for defining least privileged roles and authorisation in a multi-cloud context.
- **P5 – Manage privileged access in the Cloud**. Description: Utilise Privileged Access Management tooling for the cloud in order to prevent highly privileged accounts from causing disruptions. EMA will ensure recording and notifying when privileged access is utilised to monitor admin activities. In addition, privileged access activities will be reviewed periodically. Finally, Cloud-native services such as Just-In-Time access will be offered and required for most admin accounts.

Infrastructure security

- **P6 – Secure development artefacts**. Description: EMA will offer developers and operations secure and reusable artefacts for the maintenance and development of systems and applications. Examples are Infrastructure as code and secure virtualisation images. This also allows for automation of formal SDLC processes.
- **P7 – Leverage Software-defined Networking**. Description: Software-defined networking (SDN) allows networks in the cloud to be segmented easier and more effectively. Most CSPs also offer SDN firewalls per virtual network and subnet. This will be leveraged to decrease the attack surface of compromised assets by segmenting network assets to only necessary connections.

Application security

- **P8 – Utilise software-defined security**. Description: Whereas Secure Development artefacts offer preventive measures, they may lack in corrective and detective measures. In Cloud environments, EMA shall utilise software-defined security such as Compliance as Code solutions from CSPs. This prevents insecure configurations and automatic remediation.

Security Operations of Cloud services

- **P9 – Security Orchestration and Automation**. Description: The cloud offers many different services; it is important that these resources are also monitored and incidents are detected timely. However, due to the scale of the cloud, not all incidents might be escalated effectively or take up a lot of time. Hence, in a multi-cloud environment, EMA will consider cloud-native Security Automation and Orchestration capabilities by design around the handling of alerts and incidents in the cloud environments.

Identify responsibilities

One of the challenges of the cloud is the shared responsibility model. For information security, this entails that some controls might be the responsibility of the CSP while other controls might be the responsibility of the organisation itself. For each CSP, this shared responsibility might differ. Hence, EMA shall define the shared responsibility and adequately define which departments or teams are responsible for what controls.

The picture below highlights an example of a Shared Responsibility Model. This model highlights the different control domains and controls itself that need to be managed by the organisation and the CSP. The mix of colours highlight the shared responsibility. Each colour representing a different team.

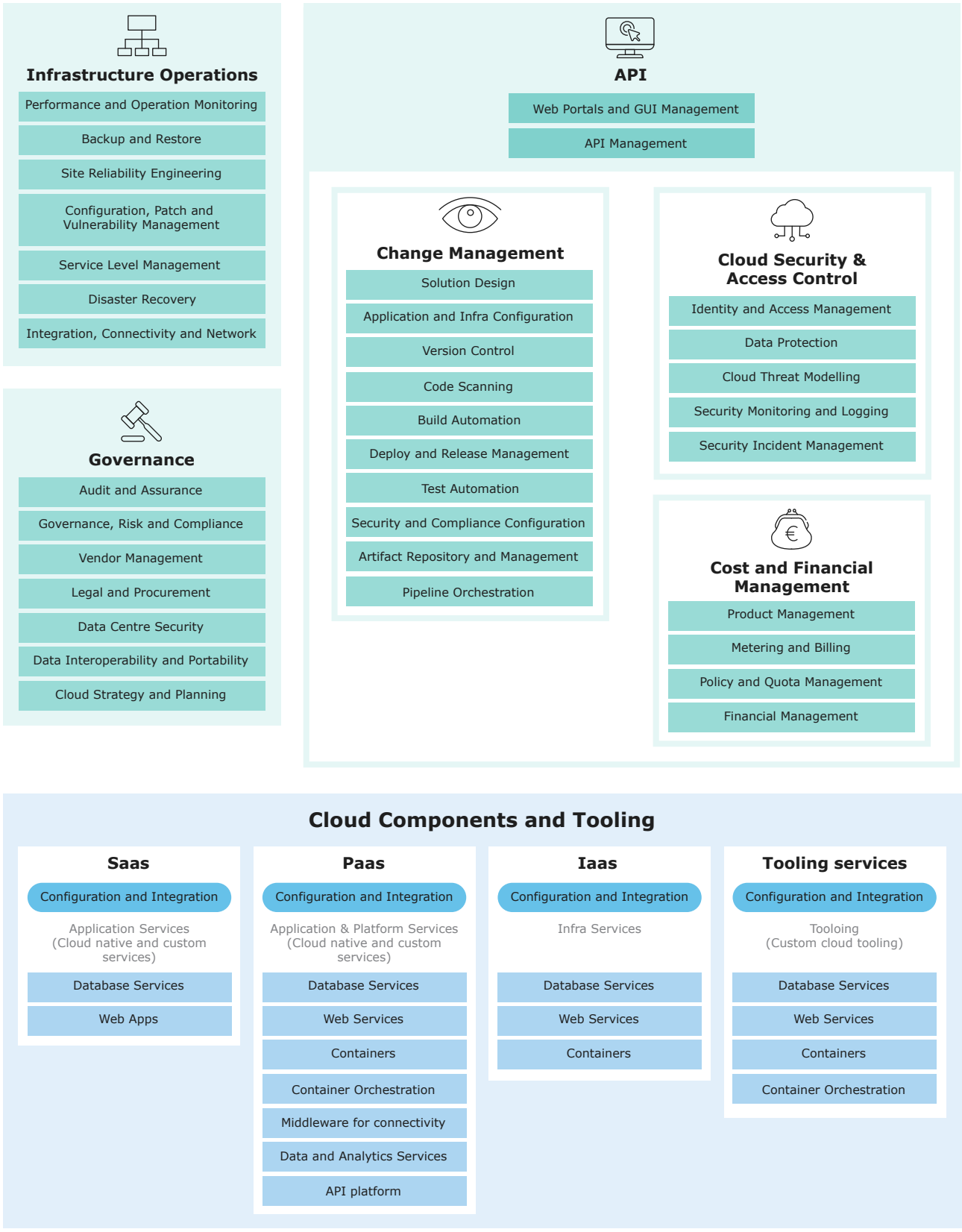
In order to determine a shared responsibility model, EMA will perform the following actions:

- Define and clarify ownership of each service across teams and the cloud service provider (CSP);
- Determine the key required stakeholders across EMA to determine accountability for the defined cloud controls based on capabilities;
- Assess current implementation of controls in existing policies and standards.

Ultimately this will be used to develop a service catalogue which outlines which team exactly does what for each control. To define this service catalogue, we define the following steps:

- Establish service catalogue to cover at least 70-80% of the commonly used cloud services (e.g., preferred storage, VM, CI/CD);
- Determine default controls commonly used cloud

Figure 10. Indicative shared responsibility model



services should have;

- Develop categories of cloud services ranging from fully secured, to not secure by default;
- Define detailed roles and responsibilities for teams per cloud service category;
- Blacklist unsecured cloud services;
- Establish a procedure to maintain and update service catalogue.

Finally, using the above, a manageable artefact is created that aims to both govern cloud controls across various teams as well as create transparency on EMA and the CSP responsibilities.

Governance and compliance

In order to manage cloud security, EMA will implement governance on four aspects:

- Cloud security policies
  - Define which data can be shared upfront and in which environment
  - What are sanctioned services for different Cloud Service Provers (CSPs)
- Tooling for Cloud
- Establish Risk assessments on Cloud
- Roles and responsibilities

Selection of vendors will follow normal procurement procedures and rules.

5. Exit strategy

When going to the cloud, an exit strategy needs to be defined in order to deal with inadequate service and other risks such as vendor lock-in. An exit here does not necessarily mean a total exit from the cloud but could mean a change of providers by ensuring portability of data or to on-premise if needed.

To define an exit strategy, several aspects will be considered:

- Analysis and scope
- Risk analysis and exit triggers
- Exit scenarios and planning

Analysis and scope

For the analysis and planning phase, the first and foremost activity that needs to be undertaken is determining the decision body that will determine when migration triggers have been reached and an exit is necessary. A migration trigger in this context might be a measurable level of (un)acceptable service or security and/or compliance. Accordingly, the scope of the exit strategy must also be determined – i.e. for which workloads and cloud hosted resources and data is the exit strategy defined?

Risk analysis and exit triggers

An exit strategy should address the strategic risks EMA may encounter while using the public cloud. In order to determine these risks, the relevant threats need to be identified. These threats may be formulated later on as the exit or migration triggers. Examples of exit triggers could be:

- Service-related, for example SLA breaches;

- Continuity-related, for example a large outage;
- Security-related, for example a large-scale hack;
- Financially related, for example a price increase;
- Strategy-related, for example the company decides to host everything on-premise again.

Ideally these triggers should be made measurable as to have a clear idea of when an exit is mandated. Once these triggers are made measurable, EMA must define the impact in terms of finances, continuity or functionality.

Exit scenarios and planning[4]

Based on the threats and subsequent estimated impact, a mitigation will be determined based on EMA's risk appetite and openness to migration complexity. Hence, EMA will define effectively the possible migration scenarios and rank select them based on costs, risk appetite and technical feasibility.

Finally, having determined an exit strategy for exit scenarios, based on several contexts and constraints, a plan may be devised to execute the exit strategy. It is important that a plan should at least contain the following:

- Technology required to run hosted applications and systems;
- People required to support the migration and future maintenance;
- Impact on business processes, costs, functionality and resiliency;
- External and internal constraints such as regulation and internal policies.

4 Deprins, T. (2021). Cloud exit planning guidelines for financial services institutions - Microsoft Industry Blogs. Retrieved 8 July 2021, from https://cloudblogs.microsoft.com/industry-blog/financial-services/2020/11/23/cloud-exit-planning-guidelines-for-financial-services-institutions/

Glossary

Multi-cloud:

Multi-cloud refers to the use of two or more cloud service providers simultaneously by a single entity. For example, if an organisation consumes both AWS services and Azure services, that organisation is operating in a multi-cloud approach.

Cloud native:

Cloud native is a method of software development which focuses on designing, building and operating applications in the cloud while ensuring that all the advantages cloud offers (scalability, agility etc.) are leveraged. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

Pay-as-you-go:

Pay-as-you-go refers to a costing model where you only pay for services you're using, for as long as you use them, without any prior commitments. In other words, you only start paying once you start using a service, and you stop incurring costs related to that service from the moment you stop using that service.

IaaS:

IaaS, or Infrastructure-as-a-Service, is a cloud computing approach where the cloud service providers only provides infrastructure to the client (e.g. storage space, networking features, VMs etc.) This provides the client with the highest level of flexibility in how to use this infrastructure and most closely resembles the on-premises way of working.

PaaS:

PaaS, or Platform-as-a-Service, is a cloud computing approach where the cloud service providers provide their clients with a 'platform' and take responsibility for managing the underlying infrastructure. This allows the clients to focus more on the applications which are running on the platform, making it easier to deploy and maintain these applications.

SaaS:

SaaS, or Software-as-a-Service, is a cloud computing approach where the cloud service provider provides their clients with a fully-fledged application which is completely managed by the CSP. As a client you simply use the application, without having to worry about anything regarding running the application. A good example of this is Microsoft Office 365.

Annexes

Enterprise strategies for migrating applications to the Cloud:

Migrating Applications to the Cloud: Rehost, Refactor, Revise, Rebuild, or Replace?, Gartner, Richard Watson, December 2020:

https://www.gartner.com/en/documents/1485116/migrating-applications-to-the-cloud-rehost-refactor-revi

Data protection references:

Guidelines on the use of cloud computing services by the European institutions and bodies, EDPS, 2018:

https://edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, EDPB, 2020:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

Deprins, T. (2021). Cloud exit planning guidelines for financial services institutions - Microsoft Industry Blogs. Retrieved 8 July 2021:

https://cloudblogs.microsoft.com/industry-blog/financial-services/2020/11/23/cloud-exit-planning-guidelines-for-financial-services-institutions/

EBA Guidelines on outsourcing arrangements, 25 February 2019:

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

European Medicines Agency

Domenico Scarlattilaan 6
1083 HS Amsterdam
The Netherlands

Telephone +31 (0)88 781 6000
Send a question www.ema.europa.eu/contact

www.ema.europa.eu

European Medicines Agency Cloud Strategy
Accelerating innovation and digitalisation for better public and animal health outcomes
EMA/214957/2022

An agency of the European Union