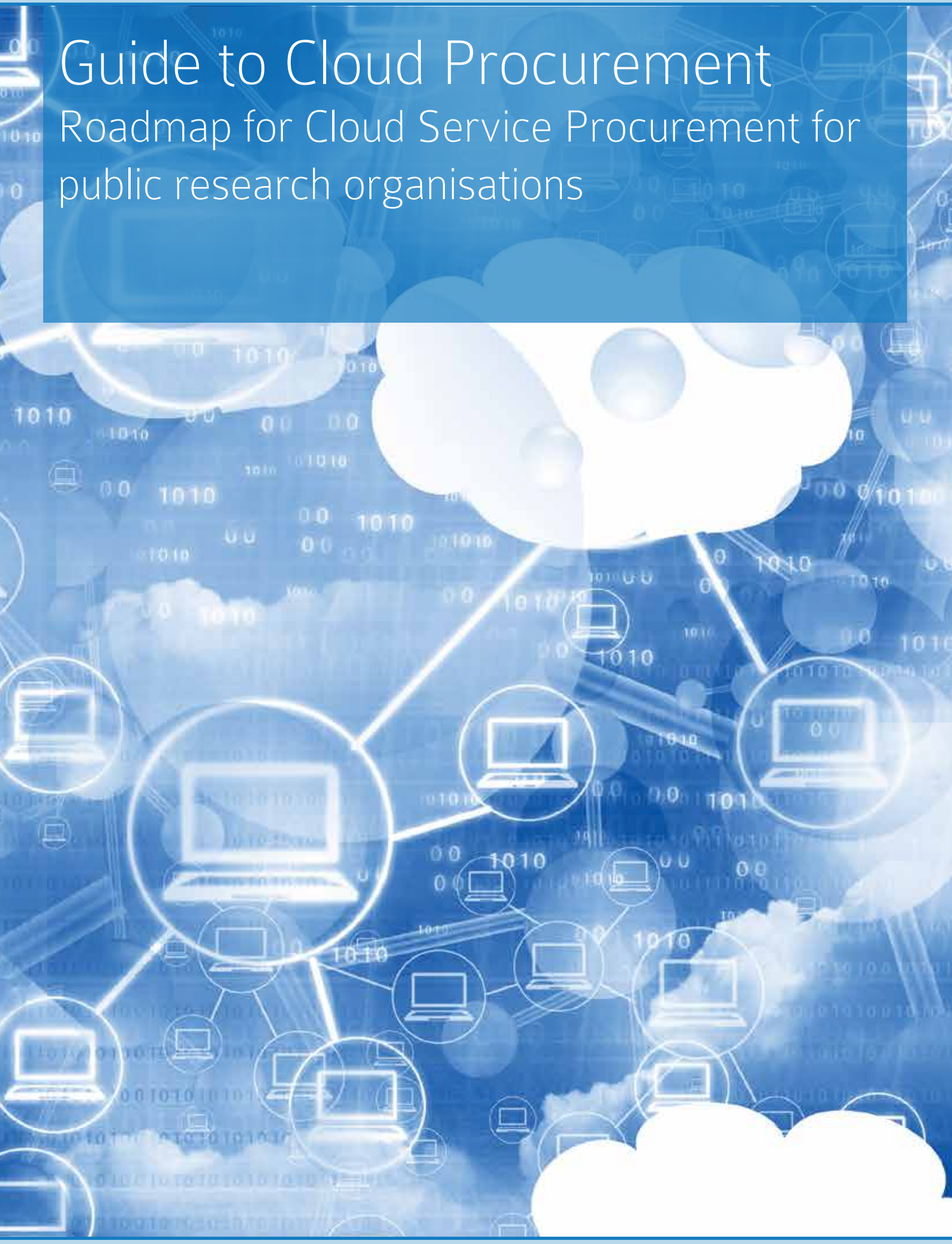
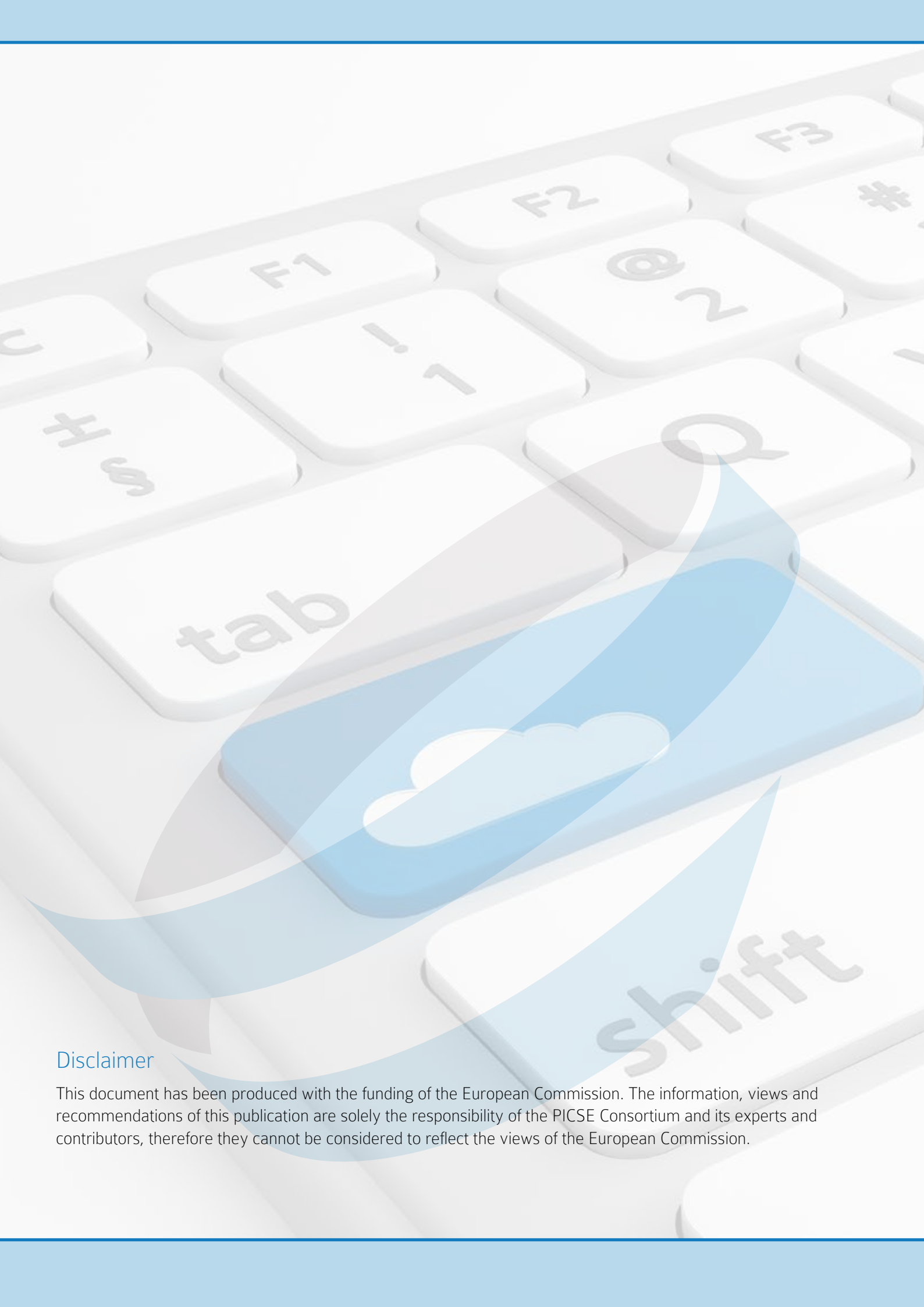
Guide to Cloud Procurement

Roadmap for Cloud Service Procurement for public research organisations





Disclaimer

This document has been produced with the funding of the European Commission. The information, views and recommendations of this publication are solely the responsibility of the PICSE Consortium and its experts and contributors, therefore they cannot be considered to reflect the views of the European Commission.

Index

Introduction 3
Identify the most suitable cloud service model for your needs 3
Understanding cloud procurement issues 4
- Understand the purpose of your procurement 4
- Make sure that the procurement process complies with public sector and in-house policies 4
- Identify the most suitable cloud deployment model for your needs 4
- Make sure you can evaluate the implications of the choice of cloud service 5
- Carry out pre-procurement market consultation & engagement 5
- Choose joint procurement to benefit from economies of scale 6
- Write an effective cloud tender 6
- Consider the need for a pilot phase 7
- Define objective eligibility criteria for Cloud Service Providers 7
- Identify technical requirements clearly 7
- Identify legal requirements clearly 7
- Identify commercial requirements clearly 8
- Assess cloud-specific Terms of Service carefully 9
- Select the most suitable procurement procedure 10
- Choose innovation partnerships if you are procuring new cloud services 11
- Write up case studies of procurement exercises to share best practice 11

Introduction

This document is not simply a 'how to' guide. Rather, its purpose is to **act as a checklist for all those involved in procurement of cloud services** including problem-owners (customers), operational staff, contract advisors and solutions providers (suppliers) to establish the extent to which their procurement practices are fit for cloud procurement. Much of the content of this checklist will be familiar to many of its readers. That is to be seen as a good thing. The next step is to consider why and how to address the concepts that are not familiar.

Identify the most suitable cloud service model for your needs

Cloud services are provided according to three different service models. NIST, the National Institute of Standards and Technology, in its special publication 800-145, "The NIST definition of Cloud Computing"[1] defines the cloud service models as follows:

IaaS (Infrastructure as a Service)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)[2].

PaaS (Platform as a Service)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

SaaS (Software as a Service)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings[3].

Practices that have worked for many years when buying conventional ICT applications and platforms may not work for commodity-level cloud services. Concepts like "value for money" or "best value" exist in the public sector as well as for private companies but there are additional considerations for public bodies in terms of their significant influence on innovation, competitiveness and social issues.

As highlighted in our four case studies in Chapter 4 of the PISCE Procurement Roadmap, there are various ways of meeting procurement requirements such as transparency and avoidance of 'lock-in'. And, of course, what works in one jurisdiction may not currently be possible under another. Many of these issues can be explored through the CloudWatch Hub[4] and there is a comprehensive set of guidelines from the Cloud Select Industry Group working party from the Safe And Fair[5] initiative. These guidelines are designed to help reassure cloud users that the Service Level Agreement (SLA) and the contract with the cloud provider meet key requirements, including:

- The availability and reliability of the cloud service being purchased.
- The quality of support services they receive from their cloud provider.
- What happens to their data when they terminate their contract.
- The security levels they need for their data.
- How to better manage the data they keep in the cloud.The service models do not all work the same way. As a result, although the Terms and Conditions for the three service models share many common clauses, those dealing with operational responsibilities vary. An SaaS service provider is responsible for data protection and encryption of data at rest whereas a PaaS provider is not (applications and data are still the responsibility of the customer, as shown in green in Figure 1).

The IaaS service provider is essentially leasing the infrastructure to the public organisation, requiring the public organisation to be responsible for its own data protection, encryption and reporting. Clauses dealing with compliance to application accessibility standards and those requiring Web services are simply not applicable to IaaS contracts.

Because SaaS providers are responsible for their customers' data, special conditions for termination and suspension of service have to be defined, which is not the case with PaaS and IaaS contracts. SaaS contracts specifically require a service provider to maintain data for up to 10 days after a contract expires in accordance with the termination timelines.

The latest trends see the rise of a fourth model, **ICT-as-a-Service**. Nearly anything that you would use a traditional computer for – such as e-mail, web browsing or word processing – will be done via the cloud at a (theoretically) lower cost and with increased reliability and productivity.

1 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

2 Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed.

3 The pricing model for SaaS applications is typically a monthly or yearly flat fee per user, so price is scalable and adjustable if users are added or removed at any point.

4 http://cloudwatchhub.eu

5 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138

	Traditional IT	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)	
Customer responsible	Applications	Applications	Applications	Applications	Service provider responsible
	Data	Data	Data	Data	
	Runtime	Runtime	Runtime	Runtime	
	Middleware	Middleware	Middleware	Middleware	
	Operating system	Operating system	Operating system	Operating system	
	Virtualisation	Virtualisation	Virtualisation	Virtualisation	
	Servers	Servers	Servers	Servers	
	Storage	Storage	Storage	Storage	
	Networking	Networking	Networking	Networking	

Figure 1: Public Sector Management of XaaS Platforms (after IDC).

Understanding cloud procurement issues

The guidelines in this document are presented as follows:

- Understand the purpose of your procurement.
- Make sure that the procurement process complies with public sector and in-house policies.
- Identify the most suitable cloud deployment model for your needs.
- Make sure you can evaluate the implications of the choice of cloud service.
- Carry out pre-procurement market consultation & engagement.
- Choose joint procurement to benefit from economies of scale.
- Write an effective cloud tender.
- Consider the need for a pilot phase.
- Define objective eligibility criteria for Cloud Service Providers.
- Identify technical requirements clearly.
- Identify legal requirements clearly.
- Identify commercial requirements clearly.
- Assess cloud-specific Terms of Service carefully.
- Select the most suitable procurement procedure.
- Choose innovation partnerships if you are procuring new cloud services.
- Write up case studies of procurement exercises to share best practice.

Understand the purpose of your procurement

What is driving your procurement? It may be cost-reduction or the need to replace capital expenditure with payment from the operational budget. It may be a capacity issue with the need to respond rapidly to variable, but predictable, levels of demand. Or it may be part of the process of flattening the organisation – replacing specialist operations (such as ingest of data for preservation) with end-user workflows using cloud-based services that can be acquired by an individual researcher. In some cases, the procurement exercise is a flagship for a whole new way of thinking, such as the various 'open science' pilots that are taking place with the support of H2020 or equivalent programmes. In others, the primary issue is the inherent flexibility of a cloud-based solution. Failure to acknowledge this flexibility means that you are procuring little more than just another 'managed service' bound by traditional SLAs.

Make sure that the procurement process complies with public sector and in-house policies

Public sector procurement is often seen as an agent for innovation and competitiveness and as a way of addressing social issues. The public sector is also subject to EU Public Procurement Directives for the advertising and the award of Contracts if the value of the contract is above a recently revised threshold (€135k for central government bodies, €209k for other public sector contracting authorities). This does not apply to commercial entities although the transparency of procurement processes afforded by the Directives is often seen as best practice in the private sector too.

Eligiblity for access to European Structural Funds may also have to be considered, since capital projects funded by ERDF have to comply with different rules to revenue projects under either ERDF or ESF.

Most if not all public sector bodies have some way of allocating budget between capital and revenue costs and ways of ensuring that costs allocated to those budget allocations are (a) actual, (b) necessary and (c) appropriate. The various funding schemes operated by the EC are good examples. One significant aspect of procuring for the cloud is that the customer is no longer puchasing hardware, software or anything else which has an upfront cost. With cloud you are procuring services.

The PICSE Wizard (wiz.picse.eu) is a web-based application designed to support public research organisations in choosing the most suitable model for procuring cloud services. The tool will help you do a self-assessment of your current procurement process and provide you with a clear set of guidelines on how to improve it.

Identify the most suitable cloud deployment model for your needs

The number of users and their location can influence the cloud deployment model and the legal aspects to be considered in a Service Level Agreement (SLA) with the vendor. Each

deployment model differs in terms of who has access to information and resources. There is a summary of key differences in Figure 2 below

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Make sure you can evaluate the implications of the choice of cloud service

Traditional procurement of ICT services consists of a pipeline of events, starting with definition of technical specifications (or of business requirements) by the IT manager responsible, typically the budget-holder. There is then a decision of whether to "build or buy", either building the solution in-house or going outside of the organisation by commissioning a bespoke application or acquiring a COTS (Commercial off the Shelf) solution. Pre-procurement market engagement can allow an open discussion of ways of ensuring market value, prior to procurement engagement.

The procurement office is responsible for the process of collecting documentation for 'going to market' if an out-of-house route is followed. This includes assembling the contract and terms and conditions, for which legal expertise is also required. This is followed by engaging the market, typically working from an in-house 'approved suppliers list' or (increasingly) from an online catalogue. Finally, the successful bidder (if one exists) is selected, typically from a shortlist of some predefined minimum number of potential suppliers, after consideration of Value for Money, Most Economically Advantageous Tender and Total Cost of Ownership. Essentially, the procurement office is responsible for the entire process, drawing on technical and legal expertise as required.

Roles in cloud procurement are essentially the same as in conventional ICT procurements but the process is not so straightforward and requires continual close collaboration between all three actors. The starting point for 'going to market' is the process of selecting the most suitable cloud service model (essentially deciding whether responsibility for the runtime environment and software remains in-house or is to be outsourced), deployment model (which determines the technical, financial and legal parameters) and the procurement approach such as using a catalogue or a cloud broker. These decisions cannot really be taken in isolation of each other.

In all cases there must be a preliminary assessment to understand technical, legal and procurement needs and identify any restrictions, limitations and regulatory requirements that apply, prior even to consideration of the service and deployment models offered by potential suppliers. It may be that additional specific legal clauses need to be used and potential suppliers must be able to agree to these.

Carry out pre-procurement market consultation & engagement

Pre-procurement market engagement enables you to consult the market and to examine alternative solutions in the market by obtaining early feedback on the feasibility of the project. It serves to understand what the market can deliver now and in the future: if the gap between needs and capabilities is too great, the procurement action may encounter some issues. Transparent market engagement can also encourage the participation of a wide range of cloud service providers (CSPs). In addition, market engagement coupled with research into the available standards is an important step in assessing which

Aspects	Public cloud	Private cloud	Community cloud	Hybrid cloud
Provisioning model	Provisioned for open use by general public	Exclusive use by a single organisation	Shared use by a specific community of organisations	Combination of two or more distinct cloud infrastructures
Costing (mode of payment)	Utility (pay per use) pricing	Capital investment for initial set-up	Cost contributed by individual organisations	Mix of public and private cloud pricing
Service Level Agreements (SLAs)	Defined by service provider	Defined by the organisation	Shared by community members	Mix of different SLAs
Possible use	Handling large variations in demand for open, non-sensitive data	Mission-critical systems / handling sensitive data	Community of organisations with shared business needs	Mixed business needs

Figure 2: Comparison table for the four deployment models. Source: Practice Guide for Procuring Cloud Services, Published by the Office of the Government Chief Information Officer, Government of the Hong Kong Special Administrative Region (November 2013)

standards are the best to include in the tender. Finally, from the pre-procurement market engagement you can understand if one commercial provider can meet your needs or you need to procure from multiple providers. Make sure to look beyond your regular suppliers and engage with small- and medium-sized enterprises (SMEs). Many of the most innovative solutions come from small-sized companies.

Pre-procurement market engagement can be done using questionnaires or surveys, written submissions, face-to-face, phone or web-based meetings, open days and supplier demonstrations. Publishing a Prior Information Notice (PIN) is key to market the tender in an appropriate way. Preliminary market consultation is not directly regulated by the EU procurement directives, although the new directives state that preliminary market consultations can be carried out provided they do not distort any later competition.

Choose joint procurement to benefit from economies of scale

Cloud service and deployment models are suitable for joint procurement where there is one single tender for all participating authorities, cost of developing specifications & contracts can be shared and combined capacity can improve purchasing conditions. If joint procurement is applied carefully, legal matters such as Data Processor Agreement negotiations only have to be carried out once. There are three critical stages to a successful joint procurement:

call for interest

Run a preliminary needs assessment and disseminate a "Call for Interest" which briefly describes the nature of the product/service to be procured, with general information on the desired characteristics, together with details of timing, the procedure and contractual arrangements to be followed. This should go to as many potentially interested public organisations as possible. Authorities should be asked to declare an interest in participation by a given date (not committing them to final participation), and to include any specific technical demands they have for the services to be procured and comments on the demands if necessary.

Select a procurement model

The organisations who decide to enter into a joint procurement must carefully evaluate the suitability of the three procurement approaches available to them - subject to national regulations. These can be termed "centralised", "decentralised" and "external".

One approach is to delegate all the procurement procedures, including the publication of the tender, responding to questions and evaluate responses to a Lead Authority. This is normally the authority initiating the procurement, or possibly the largest participating authority and the approach is suitable when participants have a history of close co-operation or other relevant experience. This 'centralised' approach is often less expensive to set up than an external entity and tenders are easier to prepare which helps keep cloud procurement processes as short as possible. See the interesting case of Cloud for Europe[6].

If the participants do not feel confident to delegate the process – perhaps because the product or service to procure is relatively complex or unfamiliar, a more 'decentralised' or collaborative approach may be appropriate, with responsibilities shared and each participant consulted at each step. For example, all participants would be part of the evaluation panel. It is important to ensure each participant' needs are addressed and more time than usual must be allowed to allow the input of all partners.

Thirdly, the procurement consortium may elect to establish a jointly owned external legal entity that provides common procurement functions on behalf of two or more contracting authorities. This can be cost-effective as a vehicle for a regional buying consortium, for example.

Select a contract type

Rather than having to complete a separate tendering exercise each time an organisation or group of organisations wishes to purchase some products or services, there is a provision for a procurement framework in the Procurement Directive (DIRECTIVE 2014/24/EU[7]) allowing one or more participating authorities to establish individual contracts with one or more cloud service provider(s) in a given period.

The 2014 EC Procurement Directive allows (but does not oblige) member states to designate "Central Purchasing Bodies" (CPBs) that act as wholesalers and intermediaries capable of operating Dynamic Purchasing Systems. A DPS is an all-electronic and flexible equivalent to a framework agreement where suppliers can join at any time without being constrained by fixed cycles as found in, for example, G-Cloud. However, it is not obligatory for the Member State to allow CPBs, and so your national procurement regulations will need to be checked.

Write an effective cloud tender

Put yourself in the provider's shoes. It is important to think about what you are asking for from the cloud vendor's perspective. The best price will be reached when a request for quotation requires exactly what a cloud vendor can offer. It is recommended to have some pre-discussions with potential providers to better understand the solutions they can offer. Potential purchasers may wish to provide performance-test software in order to independently test hardware capabilities.

Buying Infrastructure as a Service (IaaS) is similar in some ways to purchasing traditional ICT goods, although the process is often much quicker than for a typical large scale hardware procurement cycle and procurement time can be measured in months (or even less if using a catalogue) not years. Technical requirements are easier to draft and suppliers' offers are easier to understand and compare, although IaaS is a low margin, high-volume business for the supplier and some costs (e.g data removal, IP issues, data transfer costs) may be less transparent.

Provide accurate specifications, including technical, legal and commercial requirements. Vague technical specifications can be misleading and prevent providers from understanding what should be provided and what the associated implementation costs are. As cloud technologies are very dynamic and new needs could emerge during the implementation phase, specifications on potential evolution of the infrastructure are encouraged. Service contracts based on KPIs are the best way to procure IaaS cloud services. Consider splitting tenders into lots or encouraging consortia to bid, in order to make the

6 http://cloudforeurope.eu

7 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.094.01.0065.01.ENG

volumes manageable. Also, try to make the administrative needs and selection criteria for bidding manageable for smaller, newer companies.

Three specific best practices are:

a. Include all of the following in your Invitation to tender/ Request for quotation:

» The specification of needs.

» Description of the procurement evaluation process and criteria.

» An indicative amount which corresponds either to a guideline for the preparation of the price submission, or to an absolute budgetary limit of the funding available.

» The eligibility criteria for CSPs wishing to bid.

» The approach to management of risks.

» Details of the distribution of rights and obligations of the parties in the tender documents which are not part of contract renegotiation.

b. Request appropriate documentation that providers are able to supply in a timely manner. Bidders, especially small suppliers, may find it difficult to provide some documentation.

c. Provide draft contractual guidelines that enable tenderers to know the 'rules of the game' when they prepare their offers, and minimize or avoid the subsequent effort of negotiation of the contract terms.

Consider the need for a pilot phase

Moving from traditional ICT to a cloud computing model will involve significant uncertainties. The change of platform and provision will affect efficiency, and hence the amount of resources required, and cost. However, before the tasks are run it is impossible to predict the performance implications. Running benchmarks on cloud systems in a free trial can help significantly although there will be overheads for both supplier and purchaser. Starting small is one of the key success factors of a procurement action of cloud services. The inclusion of a pilot phase in the procurement action is something that has to be considered in a flexible procurement model of cloud services.

Define objective eligibility criteria for Cloud Service Providers

Procurement documents should identify eligibility criteria for Cloud Service Providers (CSPs)including:

» Any constraints on jurisdiction and applicable law of the supplier.

» Evidence of capacity to deliver required service levels (see piloting/trialling, above).

» Minimum contract duration.

» Certifications required by the procuring organization. see, for examle, the ENISA Cloud Certification Schemes Metaframework[8]. Compliance with specified standards and practices for interoperability such as Topology and Orchestration Specification for Cloud Applications (TOSCA[9]).

» Compatibility with privacy and data protection requirements in line with COM (2012) 9 "Safeguarding Privacy in a Connected World"[10].

8 https://www.enisa.europa.eu/media/press-releases/enisa-cloud-certification-schemes-metaframework

9 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca

10 http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009

Identify technical requirements clearly

Security system requirements: focus particularly on security of information/data. Too much security means more cost and more technology layers. Too little security means too little protection from malicious intent. Both are bad.

» Requirements include protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to help ensure integrity, confidentiality, and availability[11].

» Understand and document the value and security requirements for your data: the protection (including, physical, cyber, legal and personnel) you would want and expect to see from any potential supplier.

Interoperability requirements: focus on whether and how the cloud provider ensures data portability (for moving data between systems) and interoperability (when upgrading software or when migrating between two competing systems).

» Certified adherence to industry standards[12] reduces your exposure to the risk of lock-in. Ending a contract for a cloud service, whether by the cloud consumer or the cloud provider, introduces additional considerations, such as what must happen to data held by the cloud provider.

Legacy Systems requirements: focus on support for the organisation's (often large) base of legacy computing applications. They require an experienced re-engineer and the possibility to perform a standalone test. Productivity and business continuity cannot suffer during a migration.

» Organisations should create mirror systems of key legacy applications – one on the new cloud platform, another on the existing platform, and compare performance, reliability, functionality before cutting over to the cloud-based version. Also, organisations should consider moving the most critical legacy applications last.

Identify legal requirements clearly

Data location requirements: focus on compliance with justifiable jurisdiction limitations on data residence and transit between locations. Currently, some courts are holding that the legal jurisdiction over a contract dispute involving data takes place in the state where the data physically resides. Therefore, it is important to specify constraints on data storage location predicated by law, regulations, or governing policies. The contract should also outline the determination of jurisdiction and applicable law by which any legal disputes will be settled, taking into account provisions of the upcoming European Commission Free Flow of Data Initiative.

This is particularly relevant in case of cross-border procurement. When processing of personal data takes place in countries not offering adequate safeguards, both the client (controller/ exporter of data) and the provider (processor/importer) must sign the model clauses adopted by the Commission with

11 See the ENISA Security Framework for Governmental Clouds https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds and the ENISA Security & Resilience in Governmental clouds report https://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

12 See the NIST Inventory of Standards Relevant to Cloud Computing http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory and the CloudWATCH Cloud Standards Guide http://www.cloudwatchhub.eu/cloud-standards-guide .

Decision 2010/87/EU. Personal data can be freely transferred outside the EU, provided that the client verifies that:

- One of the conditions listed by article 26 is fulfilled.
- The recipients of personal data signed the standard model clauses approved by the European Commission.
- The recipient organization has Binding Corporate Rules approved by the EU Data Protection Authorities in place.

Privacy and confidentiality requirements: focus on the applicable privacy law which in the EU is the law of the Member State where the data controller is located, which means the law of the State where the cloud client resides.

- Ownership rights to data and clear access requirements have to be specified. Data Ownership refers to the legal custody, control, and/or possession of data (e.g. data custody, intellectual property, exclusion of data mining or selling, data processing ownership). In the context of cloud contracting, this section of the contract establishes the public sector's ownership of its data stored in the cloud. Cloud contracts should clearly state who owns the data residing in the cloud.

Security requirements: focus on ensuring that unauthorized parties do not obtain access to sensitive data. In that sense, security is related to privacy. Outside of specially protected sectors, it is usually up to the parties to include a security framework in the contract for cloud computing services.

- Data access control typically defines those persons in an organization who have the authority to view or retrieve organizational data housed in the cloud. Usually a public research organisation should be able to access and retrieve its data stored in the cloud at its sole discretion, including the right to access all data regardless of content creator.
- It is the buyer's responsibility to establish that the vendor's security practices satisfy any buyer-specific requirements over and above relevant legislation.
- A data security breach occurs when there is a loss or theft of, or other unauthorized access to, sensitive personally identifiable information that could result in the potential compromise of the confidentiality or integrity of data. Breach disclosure requirements should be addressed in the cloud contract and the processes and procedures to be followed in the event of a data breach, including notification requirements, timelines, detailed information about such breaches, and remediation activities should be articulated.

Data protection & privacy requirements: focus on understanding of what data you are putting in the cloud, who needs access to it and the impact of differences in legal and regulatory compliance requirements depending on the location (and thus the jurisdiction) of your data including resilient copies.

- Keep a record of what type of data is stored in the cloud. Protect personal data according to your needs and avoid sharing out data to unintended parties by ensuring only the intended recipients have access permissions if you share sensitive data with others through the cloud. Define the data protection roles between the parties as well as control rules.
- Bind the data cloud service provider, acting as a data processor, by means of a specific data processing agreement, or at least make sure that the boundaries of the data processing are clearly defined in the Cloud Service Agreement and that the activities outsourced to the cloud service provider are adequately circumscribed. The degree of autonomy left to the data processor in the choice of methods and technical or organizational measures must be defined.
- Privacy provisions for personal or confidential business information must be in accordance with applicable standards expressed in the buyer's internal policies and must also comply with relevant legislation as a key performance measure.

Identify commercial requirements clearly

Performance requirements: focus on a level of performance that is achievable, not just the minimum performance defined by SLAs. The relationship between financial incentives and well-defined and achievable performance measures needs to be understood. A contract based on delivery of minimum service levels set by the customer tend to result in the minimum necessary performance to achieve those levels because there is no incentive to improve. Put bluntly, once a suppler has met their target it is probably in their commercial interest to divert effort into other work where targets (and therefore payments) are at risk.

- Two typical performance measures are downtime and throughput. There is a world of difference in terms of impact on the customer organisation between a service that is unavailable for six hours once a year (a situation whch should be avoided by providing suitable redundancy) and one that is down for a minute every day (which is probably acceptable for many scenarios). Yet both can claim to be available for 99.9% of the time. Rather than simply paying for 'uptime', cloud-users may need to think in terms of the need for dynamic reconfiguration as a way of ensuring throughput even if demand is heavy (expressed, perhaps, in terms of wait-time before a VM becomes available).
- Disaster recovery requires a different kind of performance measure, based on mitigation of risk rather than penalties in the event of a disaster occuring. The vendor must be asked to demonstrate its redundancy provisions and regular audit checks need to be included in performance measures. This is even more critical where the vendor subcontracts to another cloud service. In these cases the vendor will need to provide an attestation that its provider has suitable disaster recovery processes.

Continuity requirements: focus on precisely specified responsibilities for all potential areas of breach in the contractual agreement. Each requirement will differ according to the nature of the data, the industry and any regulation and purpose for using the service. Arbitrary suspension of service or payment for service should be avoided and consequences of each form of breach should be addressed explicitly. This is especially important in a multi-tenant cloud where one user could compromise the service of another.

- There should be an agreed response to extended non-availability of service (based on an agreed definition and timing of downtime) such as payment suspension, which can be applied automatically. A downtime calculation needs to start precisely when services are suspended, not when the buyer notifies the vendor.
- Termination notice timeframes need to be agreed between both parties unless there is a material breach. These breach terms need to be clearly spelled out in the contract. This gives the buyer sufficient time to secure its data and seek alternative service providers.

» Liability must be capped, normally as some calculation based on the value of the contract (in total or to date) or the nature of the potential loss to the buyer, such as intellectual property.

Assess cloud-specific Terms of Service carefully

Dynamic and changing cloud services must be monitored to ensure proper performance and benefit realization. The purpose of contract management & monitoring is also to ensure the contractor is adhering to the terms and conditions of the contract and is providing the required services/products that meet the expectations of the purchaser. In addition, as cloud services are billed regularly based on usage, the user should establish processes review and approve the billing and metering of cloud services. This will ensure that billed items and usage are directly matched. Some cloud services providers offer cost forecasting tools or usage notification services. The user should take advantage of such services if they are available.

There is no standard format for the Service Level Agreements (SLAs) and other Terms of Service that form the basis for evaluation of the offers made by cloud service providers and which become part of the resulting contract. They include parameters different from those that appear in the descriptions of traditional ICT services. The greater flexibility of a cloud computing service as compared with a traditional ICT contract means the customer has to fully understand all the aspects of the terms of service. Performance management issues are discussed in the previous section on terms of service and performance monitoring. Assessment of cloud offers must include compliance with stated requirements such as the location of data placed into the cloud and the legal foundations of any contract with the provider.

Pricing

Make sure the cloud service provider (CSP) has responded with pricing breakdowns that show which requirement(s) the price relates to, this will make comparing proposals much easier. Make sure when evaluating different CSPs that pricing assurances are included in the cloud contract. These include cost per unit or contract costs, and provisions to adjust pricing downward if the identical services (including functionality, quantities, and total contract cost) are provided to other clients at a lower cost, etc. Volume discounts are frequently offered by CSPs and need to be factored into the cost comparison. One factor that affects price once the service is deployed is the risk that demand will spiral out of control. A mechanism for monitoring this may be provided by the supplier if the buyer cannot constrain the multiple individuals/groups independent use of the service.

Disposition of Data Upon Request or Termination

Data disposition refers to the procedures and processes used to destroy data when the contracting entity requests such destruction or a contract is terminated by either party. Processes and procedures for data disposition upon contract termination or organizational request should be described in the contract.

Legal Data Holds/Public Record Requests

Litigation holds and public records responsibilities are also critical and should be included in contracts for cloud services. Compliance with public records laws and legal data holds is also a core part of cloud contracts.

Compliance with laws & regulations

Contractual arrangements regarding the jurisdiction and the applicable law must be included in the Cloud Service Agreement:

» Choose a cloud service provider who guarantees compliance with European data protection law, making sure compliance is reflected in the contract, and that the roles of data controller and data processor are clearly defined;

» Avoid providers who use a complex chain of sub-contractors located outside the EU.

Terms and conditions & functionality modification

It is important to contractually codify the functionality of the services procured from the cloud provider so that any unanticipated change in functionality that interferes with the customer's ability to use the service in the way intended can be identified and resolved.

Contracts – which include the supplier's terms and conditions - should clearly regulate which services and under what conditions, including procedural ones, can be modified in the course of the provision of services. Changes that are materially detrimental to the level of a mission critical service or/and to the level of protection of personal data should be explicitly excluded in the contract.

Changes should not be implemented without giving prior notice to the client. The written agreement of the client, or at least the client's right to be notified prior to any changes to the contract, should be contractually foreseen including the right to termination inn the event of unwanted, unnoticed and/or detrimental amendments to the contract.

Many cloud contracts incorporate standard terms and conditions by reference to the relevant URL at the cloud service provider's web-site.The terms and conditions that apply at the time of contract signature should be incorporated as an exhibit for future reference purposes in case the published terms and conditions are updated.

Contract renewal and termination

Termination of cloud computing contracts is a critical phase because it initiates a process in which the client must be able to retrieve the data transferred to the cloud, within a specified period of time, before the provider irreversibly deletes them. This phase, if not managed properly can also be costly. The steps of the termination process must be clearly identified in the cloud service agreement between the parties. A good cloud service agreement would contain provisions regulating the data retrieval time, the data retention period as well as the procedures followed by the provider in order to transfer personal data back to the client or to allow the latter to migrate to another provider. Exit strategies when moving to the cloud should be carefully defined to avoid vendor lock-in.

Select the most suitable procurement procedure

As cloud services evolve rapidly, shorter procurement cycles are envisaged. The selection of the most appropriate procurement procedure usually depends on a number of issues: the type and size of the procuring organization; the value and complexity of the procurement action; the budget and the competences available to conduct the procurement; etc. The most common public procurement procedures are the open or restricted procedures although regulations have been updated with the adoption of the EU Public Contracts Directive (2014/24/EU) which introduces many changes, summarised in a Brief Guide by the UK Crown Commercial Service[13] which gives updated definitions of the expected use of each procedure:

The new Directive introduces a new Innovation Partnership procedure and simplifies the scope of the existing Competitive Dialogue and Competitive Negotiation. The options are:

- The Open procedure, under which all those interested may respond to the advertisement in the OJEU by submitting a tender for the contract.
- The Restricted procedure, under which a selection is made of those who respond to the advertisement and only they are invited to submit a tender for the contract.
- The Competitive Dialogue procedure, under which a selection is made of those who respond to the advertisement and the contracting authority enters into dialogue with potential bidders, to develop one or more suitable solutions for its requirements and on which chosen bidders will be invited to tender.
- The Competitive Negotiation procedure under which a selection is made of those who respond to the advertisement and only they are invited to submit an initial tender for the contract. The contracting authority may then open negotiations with the tenderers to seek improved offers.
- The Innovation Partnership procedure, under which a selection is made of those who respond to the advertisement and the contracting authority uses a negotiated approach to invite suppliers to submit ideas to develop innovative works, supplies or services aimed at meeting a need for which there is no suitable existing 'product' on the market. The contracting authority is allowed to award partnerships to more than one supplier.

In certain narrowly defined circumstances the contracting authority may also award a contract using the 'negotiated procedure without prior publication'. Here the contracting authority would approach one or more suppliers seeking to negotiate the terms of the contract. One of the permitted circumstances is where, for technical or artistic reasons or because of the protection of exclusive rights, the contract can only be carried out by a particular supplier.

Contracting authorities have a free choice between the open and restricted procedures. The competitive dialogue procedure and the competitive procedure with negotiation are available where certain criteria are met, including where the contract is complex or cannot be purchased 'off the shelf'. The 'negotiated procedure without prior publication' may only be used in the limited circumstances described in the Public Contracts Directive.

The key features of each of the procedures, including the new Innovation Partnerships, are shown below.

Notes on specific provisions:

- All tenders over specified value must be advertised in OJEU. Lower-value tenders may optionally be advertised.
- All procedures except the Open procedure use a pre-qualification step to reduce the number of potential suppliers that have to be considered for shortlisting. The minimum number of shortlisted suppliers is three (or five in the case of the Restricted procedure).
- In the Open and Restricted procedures, potential suppliers submit their responses to the tender documentation. These are assessed and the supplier chosen.
- In the Competitive Consultation procedure a structured dialogue is used to clarify key points prior to issuing a final tender document.

Process steps		Open	Restricted	Competitive	Negotiated	Innovation Partnership
Award	Procurer selects against criteria	y	y	y	y	
Negotiation	Procurer negotiate terms of contract with (suppliers)	n	n	n	y	
Final tender	Supplier responds to revised invitation to tender	n	n	y	n	
Dialogue	Procurer enters into dialogue with shortlisted suppliers	n	n	y	y	
Tender	Supplier responds to tender documents	y	y	y	y	
Shortlist	Suppliers selected for shortlist on basis of PQQ	n	y	y	y	
PQQ	Supplier completes a pre-qualification questionnaire	n	y	y	y	
Specification	Publication of the advertisement	y	y	Y	Y	

13 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/472985/A_Brief_Guide_to_the_EU_Public_Contract_Directive_2014_-_Oct_2015__1_.pdf

» In the Negotiated procedure, the structured dialogue and tendering process of competitive consultation is replaced by a more flexible approach, the use of which is limited to very specific circumstances.

Choose innovation partnerships if you are procuring new cloud services

Innovation partnerships are new procurement models that address two obstacles to adoption of innovation in products and services. These can work well for more sophisticated forms of cloud procurement such as PaaS / SaaS. The first step is to stimulate R&D that can result in competing approaches to problem-solving so that they can be evaluated and the most promising prepared for introduction to the market. This is addressed by the PCP mechanism. The second step is to encourage adoption of those new-to-market products and services through a PPI project.

Pre-Commercial Procurement (PCP) is an approach for procuring R&D services, in three phases prior to the availability of goods and services: solution exploration, prototyping and test implementation. This enables public procurers to:

» Share the risks and benefits of designing, prototyping and testing a limited volume of new products and services with the suppliers, without involving State aid.

» Create the optimum conditions for wide commercialization and take-up of R&D results through standardization and/or publication.

» Pool the efforts of several procurers.

Public Procurement of Innovative Solutions (PPI) is a mechanism that can create demand long before a commercial market is established. This has three key advantages:

» By acting as the first buyer or lead customer, a public sector procurer can boost a specific new market.

» This provides a mechanism for stimulating market interest in the results of PCP. Together, PCP and PPI can lead to scientific and technological breakthroughs in areas such as health and well-being, food security, sustainable agriculture or clean & efficient energy.

» New and innovative public services can be provided in a more cost-efficient and effective manner by the use of more mature solutions.

The most complex aspect of the PCP/PPI instruments is the potential that exists for conflict with state aid and public procurement law. Communication 799 (2007) makes the case that PCP does not constitute state aid and that R&D was excluded from the public procurement Directives (Art 16f of 2004/18/EC, Art 24e of 2004/17/EC). Although these have now been replaced by Directive 2014/24/EU and Directive 2014/25/EU, COMM 799 still applies to PCP. PPI is regulated by these new public procurement Directives and Directive 2014/23/EU.

The way intellectual property is to be exploited must comply with relevant law (see above). PCP/PPI involves an investment in making new ideas a reality, both by the contracting authority and the supplier(s) or service provider(s) involved. Each will want to recoup its investment, and this often takes the form of asserting intellectual property rights (IPR). In order to capture the benefits of innovation which are most important to it, without paying unnecessarily for rights and options which won't be used, the contracting authority should develop a strategy on IPR which takes into account the likely future applications of the product or service it is purchasing. IPRs resulting from a PCP are not exclusively reserved to the procurers, but shared between procurers and bidders. Recommendation: ownership assigned to bidders and use/development rights assigned to procurers, through licences and sublicences scheme, and just for purposes linked to the procurers public mission and within their territorial scope.

Three considerations for successful PCPs and PPIs:

1. In PCP and PPI the dialogue with industry is fundamental in obtaining an overview of the state of the art and of the available technologies.
2. Accurately define risks and responsibilities: Buying innovative solutions will inevitably entail a certain amount of risk, whether technical or financial. It is important to carefully consider what those risks might be and to make sure that it is clearly defined who is responsible for carrying that risk, and that this be clearly included within tendering and contract documents. A piloting phase can help to substantially reduce risk[14].
3. The award of a PCP/PPI cannot be based on lowest price only. The PCP/PPI contracts shall be awarded to the tenders offering the most economically advantageous tender, taking into account other factors than price (e.g. quality).

Write up case studies of procurement exercises to share best practice

It is important to draw lessons for future procurement from each procurement process and to share best practice and lessons learned. The PICSE report "Procuring cloud services today: experiences and lessons learned from the public sector"[15] provides several case studies. The effect of using certain standards or other technical specifications can be assessed, as well as the accuracy of any cost benchmarking exercises. This evaluation can also be used to assess suppliers in the market in terms of the extent to which they have met required technical specifications in their products or solutions.

14 https://www.innovation-procurement.org/fileadmin/editor-content/Guides/Intellect_Property_Rights_guide-final.pdf

15 http://picse.eu/news/new-report-experiences-and-lessons-learned-the-public-sector-procuring-cloud-services-today


ctrl
alt

European Commission

This project has received funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 644014