PICSE: Procurement Innovation for Cloud Services in Europe

Funded under the EU Framework Programme for Research and innovation H2020 - Grant Agreement no: 644014

Deliverable Title: D3.2 Procurement Best Practices Report

Submission Due Date: M16 (January 2016)

Actual Submission Date: 07 January 2016

Work Package: WP3

Responsible Partner: CSA

Distribution: Public

Nature: Report

Abstract: This report includes a collection of procurement good practices in the public sector, both in Research and Public Administration, which cover real life examples in Europe as well as outside the EEA (e.g. in the USA). A comparison between procurement practices in the public and private sector as well a description of how current practices can overcome barriers and the identification of unaddressed challenges.

DOCUMENT INFORMATION

Project	
Project acronym:	PICSE
Project full title:	Procurement Innovation for Cloud Services in Europe
Project start:	1 October 2014
Project duration:	18 months
Call:	ICT-35-2014: Innovation and Entrepreneurship Support
Grant agreement no.:	644014
Document	
Deliverable number:	D3.2
Deliverable title:	Procurement Best Practices Report
Author(s):	Cloud Security Alliance
Work package no.:	WP3
Work package title:	Competence
Work package leader:	Cloud Security Alliance
Work package participants:	CERN, CSA, Trust-IT, PICSE Task Force
Distribution:	Public
Nature:	Report
Version/Revision:	V1.5

DISCLAIMER

PICSE (644014) is a Coordination and Support Action funded by the EU Framework Programme for Research and Innovation Horizon 2020. The PICSE Procurers' Platform will give access to a unique repository of information supporting the move from outright purchase to 'pay-per-usage' made possible by the arrival of cloud computing. It builds on the Helix Nebula collaboration between supply and demand of which the three PICSE partners are key members.

CHANGE LOG

Issue	Date	Description	Author/Partner
0.1	23/10/2015	Document structure and Initial Content	Damir Savanovic, CSA
0.2	28/10/2015	Internal review	Jesus Luna, Daniele Catteddu, CSA
0.3	29/10/2015	Feedback integration	Damir Savanovic, CSA
0.4	3/11/2015	Review from CERN	Rachida Amsagrhrou, CERN
0.5	4/11/2015	Feedback integration	Damir Savanovic, CSA
0.6	05/11/2015	Review from TRUST-IT	Sara Garavelli, Trust-IT
0.7	13/11/2015	Feedback integration	Damir Savanovic, CSA
0.8	16/11/2015	Review from CERN	Bob Jones, CERN
0.9	20/11/2015	Feedback integration	Damir Savanovic, CSA
1.0	22/12/2015	Task-Force Feedback integration	Damir Savanovic, CSA
1.1	23/12/2016	Internal review	Daniele Catteddu, CSA
1.2	7/1/2016	Feedback integration	Damir Savanovic, CSA
1.3	31/1/2016	Final draft version	Damir Savanovic, Daniele Catteddu, CSA
1.4	11/2/2016	Review from CERN, TRUST-IT	Bob Jones, CERN Sara Garavelli, TRUST-IT
1.5	22/2/2016	Final version	Damir Savanovic, CSA

Table of Contents

List of Figures

List of Tables

Executive Summary

The acquisition of IT services is a key function within any public or private organisation and the advent of cloud computing requires innovation in the way IT services are procured.

This report identifies and documents best practices for procuring cloud services in public research organisations. Because of the commonalities of the procurement practice in public administration, it was also included in the report.

While growing demand for computing power from the scientific community has resulted in initiatives such as Helix Nebula (www.helix-nebula.eu), procurement policies, processes and approaches in many research organisations are inadequate for addressing the on-demand model of cloud computing, introducing barriers to the procurement of cloud services. Such barriers have been identified, described and analysed in previous PICSE deliverables; i.e. D2.1 (Research Procurement Model) and D3.1 (Procurement Barriers Report).

To overcome those barriers PICSE has consulted ten public sector organisations across Europe, which have either already carried out a cloud service procurement action, or are considering doing so, in order to better understand what worked well in their procurement experiences (the results are documented in the PICSE brochure entitled "Procuring Cloud Services Today"). Additionally, the procurement approaches of the Crown Commercial Service (G-Cloud) in the UK, the Internet 2 Net+ initiative and the General Services Administration, both in the USA, have also been studied.

The report documents the procurement best practices to adopt in the areas of policy and organisation, processes, staff, tools and cloud service providers. The case studies considered showed that not all barriers are adequately addressed. Current internal policies and procurement rules within European public research organisations do not facilitate the procurement of cloud services. Many organisations lack cloud computing training and awareness. Contract termination and the use of cloud escrow are still to be properly addressed. Moreover, a systematic approach to defining security requirements is lacking, SLAs are not mature enough and limited only to performance measurement. Similarly, privacy and data protection provisions are usually stated within technical requirements even though they remain one of the main barriers to cloud adoption.

On the bright side, cloud marketplaces and brokerage models allow customers to buy commoditised cloud solutions in a transparent manner, offering a catalogue of cloud services, transparent cloud pricing and standard cloud contracts. Use of CSA CCM and ISO/IEC 27001 are the most common approaches for defining security requirements during the cloud procurement process and a lot of effort is being put in developing guidance and templates for SLAs related to performance, security, data management and privacy. The Internet2 CloudProud program and certifications such as CCSP from CSA and (ISC)²®, are examples of how the identified skill gap in the procurement of cloud services can be addressed.

1. Introduction

With the advent of cloud computing, the delivery of Information and Communications Technology (ICT) services is going through a fundamental change. IDC's baseline scenario for 2020 shows the total European Public Cloud market to be worth some €32.7bn[1].

The Digital Agenda is Europe's strategy for a flourishing digital economy established by 2020. It outlines policies and actions to maximise the benefits of information and communications technology (ICT) for everyone in Europe. Digital and technology are fast-paced industries. The general industry trend is moving towards focusing on delivering small, and manageable technology projects rather than mega-projects that are inherently more risky and therefore more likely to fail.

Traditional public procurement is at odds with where technology is heading today. Volume deals and longer contracts reduce costs, but also lead to vendor lock-in, which is estimated to cost the EU €1.1bn per year. As well as increasing cost, it reduces the base of suppliers available, prevents new and innovative companies from providing alternative solutions and causes the market to stagnate.

Action 23[2] of the Digital Agenda aims to provide guidance on ICT standardisation and public procurement. The Commission has drawn up detailed guidelines[3] on how to make best use of ICT standards in tender specifications. More information on open procurement practices and other different examples/initiatives related to the procurement of ICT goods and services by public bodies throughout Europe can be found in the Best Practices e-Library[4].

The EU Commission's priority is to bring down the barriers to unlock online opportunities through the Digital Single Market strategy[5]. In a Digital Single Market, there are fewer barriers, and more opportunities: it is a seamless area where people and business can trade, innovate and interact legally, safely, securely, and at an affordable cost, making their lives easier. The strategy includes 16 initiatives to be delivered by the end of 2016 and are built on three pillars:

1. Access: better access for consumers and businesses to digital goods and services across Europe;
2. Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish;
3. Economy & Society: maximising the growth potential of the digital economy.

Growing demand for computing power from public research organizations has resulted in initiatives such as Helix Nebula[6], a partnership between public research organizations and cloud service providers in Europe that is charting the course towards the sustainable delivery of cloud computing to public research organizations. However, public cloud computing as a delivery method for ICT services is disrupting the

[1] Uptake of Cloud in Europe, IDC, 2014 http://ec.europa.eu/digital-agenda/en/news/final-report-study-smart-20130043-uptake-cloud-europe
[2] https://ec.europa.eu/digital-agenda/en/pillar-ii-interoperability-standards/action-23-provide-guidance-ict-standardisation-and-public
[3] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2326
[4] https://joinup.ec.europa.eu/community/open_standards_ict/og_page/best-practices-library
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
[6] http:// http://www.helix-nebula.eu/

traditional notions of information technology. Procurement processes and policies in many research organisations are inadequately addressing the on-demand model of cloud computing, introducing barriers to the procurement of cloud services. This matters because on-demand cloud computing allows the long-tail of small-scale scientific researchers to compete across Europe on a level playing field with those who have historically secured the large research grants to invest CAPEX in their own datacentres.

This report identifies and documents best practices for procuring cloud services in the public research organisations. While the report focuses on the research sector, we considered also the procurement practices of cloud services in public administration. This is because public administrations and agencies are large consumers of ICT, and via their purchasing power can wield significant influence on innovation and competition in the ICT market. The procurement of ICT by public organisations also represents a significant expenditure of public funds. It is therefore paramount that public bodies know how to procure ICT efficiently and responsibly, promoting competition and innovation in the ICT industry and exploiting public funds to the fullest.

The work done in this report builds on the following sources:

1) Analysis of good practices in public research organisations and public sector, performed in D2.1 Research Procurement Model[7],
2) Analysis of procurement barriers identified in D3.1 Procurement Barriers Report[8],
3) Analysis of 10 cloud procurement case studies described in the report "Procuring Cloud Services Today"[9]
3) Insights and knowledge gained from the Helix Nebula flagships,
4) Information obtained from the Cloud for Europe project,
5) Crown Commercial Service (CCS) G-Cloud Framework[10],
6) Internet 2 / Net+ Initiative[11],
7) US General Service Administration (GSA) and FCCI, FedRAMP[12], BuySMART[13] initiatives,
8) Information provided by Industry Associations (e.g. DigitalEurope), and
9) Various other sources including those proposed by the Procurers' Network and the PICSE Task Force.

This report compares procurement approaches in different sectors and different geographies with a particular emphasis on the way they address the type of barriers identified in the "D3.1 Procurement Barriers Report". This report highlights potential future challenges and proposes a procurement best practice suitable for the European Scientific Community in the light of those challenges. Furthermore, it helps understand how the best practice fits and supports the work done by the PICSE consortium in the report "D2.1 Research Procurement Model". Finally, it provides input to the PICSE Procurement Roadmap (D 2.3). The best practices documented in this report also validate the procurement practices in the PICSE Wizard, a web-based application developed by the PICSE project, which public research organisations can use to obtain guidelines

[7] http://www.picse.eu/publications/deliverables/d-21-research-procurement-model
[8] http://www.picse.eu/publications/deliverables/d31-procurement-barriers-report
[9] http://picse.eu/publications/deliverables/procuring-cloud-services-today-report-experiences-and-lessons-learned-the
[10] https://www.digitalmarketplace.service.gov.uk/g-cloud/framework#the-g-cloud-framework
[11] http://www.internet2.edu/vision-initiatives/initiatives/internet2-netplus/
[12] http://www.gsa.gov/portal/category/102375
[13] http://www.gsa.gov/portal/content/105119

on the most suitable model for procuring cloud services, and to self-assess and evaluate their procurement procedures[14].

[14] wiz.picse.eu

2. Scope and Objectives

The main scope of this report is to document the cloud computing service procurement best practices in public research organisations. Since there are commonalities between procurement practice used by public research organisations and public administrations, the scope of this work was extended so as to include also public administrations and agencies. It should be noted that the same approach has been adopted in previous PICSE deliverables (e.g. D2.1 and D3.1). The analysis of cloud procurement practices in public research organisations and public administration was performed in D2.1 and analysis of barriers in procurement of cloud services were identified in D3.1.

The focus is to describe best practices in public research organisations and public sector, building on the input from D2.1 and D3.1. Another objective of the present report is to address the barriers identified in D3.1 from both private and public sectors (including the research domain), in and beyond Europe and to validate the procurement guidelines on the procurement models used in the PICSE Wizard[15], a web-based application that promotes the procurement models described in deliverable D2.1 .

More detailed objectives of this study are:

- To develop a collection of procurement best practices in the public sector, both in Research and Public Administration, which would cover real life examples in Europe as well as outside the EEA.
- To perform a comparison between procurement practices in the public and private sector.
- To provide a description of how current good practices can overcome barriers, and to identify unaddressed barriers.
- To support the goal stated in the European Cloud Computing Strategy which calls for a framework of standards to assert procurers' confidence that they have met their compliance obligations and that they are provided with an appropriate solution to fulfil their needs.

[15] http://wiz.picse.eu/

3. Target Audience

With the increasing IT needs for research and innovation, local, national and European public research organisations are moving their applications into the cloud along with their data. This means that many of them are either procuring, planning to procure or building cloud services with a view to forming a hybrid cloud with procured cloud services.

This report will help public research organisations and public administration to identify cloud procurement best practices and better understand the current barriers in procuring cloud services, which those best practices are addressing. In particular, the key actors in the procurement of cloud services listed below are part of the target audience for this report.

Procurement Initiator

The individual nominated by the management, usually with a technical background who has the responsibility, the technical competences and the budget to undertake one (or more) procurement(s). He/she is the coordinator of the whole procurement process and responsible for achieving the support and buy-in of all stakeholders for the procurement process. He/she usually works in close collaboration with technical officers, procurement, contracts, and legal experts. He/she is charged with verifying that there is a corresponding approved programme and budget within its organisation, before starting the procurement action. He/she should have a strategic overview of the needs and of the procurement action.

Technical Officer (IT manager)

A Technical Officer has the ICT background to understand the needs and the different solutions available. He/she usually also has a good understanding of the market and usually plays a role in the suppliers' identification.

Procurement Officer

The procurement officer is the person who has a complete understanding of the procurement strategy and procedures of the organisation. He/she is responsible for the identification of potential suppliers, the procurement process (tender, price enquiry, etc.), the selection of a preferred supplier, the contract negotiation, the management of a contract, and purchasing processes.

Policy Makers

Policy makers are the bodies with the power to influence or determine policies and practices at an international, national, regional, or local level.

Cloud Service Provider (CSP)

Cloud Service Provider (CSP) is the ICT vendor.

4. Methodology and Approach

This qualitative study leveraged literature review and targeted interviews.

The literature review was restricted to English language documents, with a focus on the timeframe 2011-2015, since Cloud Computing has reached maturity relatively recently and continues to evolve at a rapid pace.

An extensive review of the available and relevant Procurement best practices literature uncovered documents such as an assessment and evaluation report, recommendations and research studies on Procurement, etc. which provided insights on how to build procurement best practices.

All relevant literature is reported in the References section at the end of this report.

The research methodology followed can be summarised in the following stages:

1. Identification of good practices in procuring cloud services through extensive literature review
2. Analysis of the information coming from the target interviews performed to produce D3.1 Procurement Barriers Report and the brochure entitled "Procuring cloud services today"[16]
3. Targeted interviews with UK Crown Commercial Service, Internet2 and US General Services Administration
4. Consultation with the PICSE Task Force members
5. Organisation of targeted workshops & participation to targeted events to discuss good practices
6. Presentation of results

[16] The complete interviews will be made available in Deliverable D2.2 Research Procurement Case Studies that will be delivered on month 15.

5. Approaches and barriers to the procurement of cloud services

Section 5.1 gives an overview of the procurement barriers from the D3.1 Procurement Barriers Report and the main challenges from the case studies, while section 5.2 gives an overview of current approaches from the case studies, desktop research and targeted interviews. Section 5.3 compares public procurement practices with private procurement.

5.1 Procurement Barriers

The adoption of cloud computing services is inhibited by several factors; including barriers related to procurement, perceived trustworthiness, technical standards and legal terms of reference, risk of vendor lock-in, and many more. Potential cloud customers in the research area and across public sector are often frustrated when they try to use cloud services as and their organisation is unwilling/unable to make the organisational changes necessary for the effective use of cloud services.

The overall challenge is to overcome these barriers in order to boost the public research organisations' productivity by stimulating the preparedness for wide adoption of competitive, secure, reliable and integrated cloud computing services.

The following list of procurement barriers to the adoption of cloud services has been curated from the outcomes of the D2.1 Research Procurement Model and the D3.1 Procurement Barriers Report.:

- Lack of skills and competences: All actors involved in the procurement process should have a sufficient understanding of the new technology being purchased.
- Organisational/cultural barriers: Change management strategies and the setup of new governance mechanisms should be taken into account at the time of procurement, as they may incur additional costs.
- Cloud business case: Financial issues associated with new cost evaluation methods may arise. It is both important and also challenging to carry out a business case in order to understand how cloud computing fits or does not fit with the strategic business goals of the organisation. Short-, medium- and long-term cost savings and efficiency gains should be considered, bearing in mind the exchange of one set of risks for another. Furthermore, not all public research organisations have sufficiently detailed accounting models to permit a comparison of costs between in-house provisioning and external procurement.
- Legal-organizational barriers:
    - Applicable law
    - Data location restrictions refer to explicit or legal requirements to keep data on site or within national borders
    - Data protection is the major barrier when processing personal data
    - Lawful access - ensuring that data is accessible on court order, at the same time not having data seized by foreign authorities on the grounds of physical location of data
    - Procurement issues arise from the current procurement law not matching "take-it" or "leave-it" paradigm of cloud contracts

- Lack of information security assurance
- Data protection/privacy
- Data and service portability
- Interoperability
- Vendor lock-in, vendor liability and confidentiality assurance are aspects that have to be considered.
- Performance monitoring: Dynamic and changing cloud services must be monitored to ensure proper performance and benefit realization. Service level agreements (SLAs) must be drafted and managed properly.
- Service customisation and contractual flexibility: those are two important barriers identifies by the users. As contract negotiation is critical and there are no standard contracts for cloud computing, contract termination conditions need to be carefully evaluated. Cloud escrow is also a missing point.

5.2 Existing Procurement approaches

PICSE has consulted the various public research organisations and public administration (both European and American) in order to capture the current state and approach to the procurement of cloud services. This consultation identified a set of relevant good practices:.

- ***European intergovernmental organisations*** (e.g. CERN[17], ECMWF[18], EMBL[19], and ESA[20]) are large-scale scientific organisations governed by member states and subject to their own legislation. Member states decide the overall procurement strategy of the organization and also establish the threshold for public tender. They usually have a procurement office in charge of the procurement action and strict, formal rules. They are often equipped with a supplier database that includes all of the eligible suppliers. Suppliers entering this database have to pass a formal evaluation process in which they demonstrate their compliance with the rules of the organization. Criteria include geographical constraints (usually only suppliers from the member states funding the organization can be considered eligible), size (SMEs are often considered risky suppliers), and certifications, etc.
- ***National research institutes*** (e.g. Umea University, and CNR) including large/medium and small-scale universities or research centers funded only by the member state in which they are located. These institutes must comply with national legislation and therefore, legal implications on procurement procedures are simpler. A procurement office may be within the institution although it depends on the size of the organization. In smaller institutes this role is often covered simply by a legal expert who together with the technical officer is in charge of the procurement action. As for inter-governmental organisations, each institute has its own procurement rules and procedures.

[17] home.web.cern.ch/
[18] http://www.ecmwf.int/
[19] http://www.embl.de/
[20] http://www.esa.int/ESA

The PICSE brochure on "Procuring cloud services today"[21] describes the experience of ten public sector organisations across Europe, which have either carried out a process to procure cloud services, or are considering doing so. The experiences vary in terms of success and offer insights into how the procurement of cloud services is impacting on their current processes. PICSE has expanded the analysis of current European procurement approaches looking into the procurement approach of Crown Commercial Service (CCS) in the UK and procurement approaches of Internet 2 Net+ initiative in the USA and of the US General Service Administration.[22]

5.2.1 The G-Cloud framework

The G-Cloud Framework Agreements allow public sector customers to buy commoditised cloud based solutions through a framework that is compliant, regulated and regularly updated allowing G-Cloud to provide their customers with off-the-shelf, pay-as-you-go, up-to-date innovative cloud solutions. The Digital Marketplace[23] is the online catalogue which transparently showcases all services available through the G-Cloud Framework. The supplier on-boarding process is comprised of 5 mandatory steps, providing supplier's service information, including service definitions, pricing, and terms and conditions. The Digital Marketplace offers 21,000+ services across four lots: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Specialist Cloud Services, offered by 1,900+ suppliers, 87% of whom are small and medium enterprises (SME). The G-Cloud buying process provides its customers with a more time and cost effective buying process as no publication in the Official Journal of the European Union (OJEU), invitation to tender (ITT), request for price (RFP), request for quote (RFQ), and request for information (RFI) or negotiation are needed. For further details see Annex 1.

5.2.2 Internet2 NET+ program

Through NET+, the research and education (R&E) community in the USA is procuring its own cloud services and applications, tailored to its own broad user community. Through Internet2 NET+ partnerships, commercial cloud solution providers tailor offerings to meet shared R&E needs. Through a rigorous, peer-driven evaluation process, R&E institutions and cloud service providers work together to develop solutions that maximize deployment efficiencies and minimize business and legal challenges, financial costs, and the technological risks in migrating on-campus into cloud-based solutions. Members collectively identify and vet cloud solutions that the community believes can be effective in fulfilling challenges, and have the potential to scale, meeting the needs of all the research institutions. NET+ services are made broadly available only after they pass this peer-driven service evaluation process. At that point, new business models, legal agreements, and the best possible pricing and terms for all are created to accelerate adoption and implementation. Leveraging the collective technical and functional expertise of Internet2 members, combined with the collaborative scale of the R&E community ensures that Internet2 NET+ services are high-value, collegially vetted, ready-to-use cloud solutions, simple to access and administer, and tailored to the unique needs of R&E. For further details see Annex 2.

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

[22] With regards to procurement practices we have noted that a number of universities already perform joint procurement for ICT equipment and services without the engagement of the European Commission (EC). For example:

- The Higher Education Purchasing Consortium, Wales (HEPCW): http://www.hepcw.ac.uk/
- London Universities Purchasing Consortium (LUPC): http://www.lupc.ac.uk/

Such consortia could be encouraged to jointly procure cloud services and engage in EC co-funded PCP/PPI actions.

[23] https://www.digitalmarketplace.service.gov.uk/

The main benefits of NET+ program are:

- Cost Control
  - Lower pricing
  - Lower procurement cost/effort
- Enhanced Value
  - Favorable terms
  - Better alignment with local IT architecture
- Future Proofing (lower risk)
  - Strategic engagement with provider at community scale

5.2.3 US General Services Administration

The US General Services Administration[24] (GSA) serves as a centralized procurement and property management agency for the federal government. Cloud services are usually offered and purchased as commodities. The Federal Risk and Authorization Management Program[25] (FedRAMP) was developed as a government-wide initiative to provide joint authorizations and continuous security monitoring services for all federal agencies with an initial focus on cloud computing. FedRAMP allows agencies to use or leverage authorizations. Under this program, agencies are able to rely upon review security details, leverage the existing authorization, and secure agency usage of system. This greatly reduces costs, enables rapid acquisition, and reduces effort. The SmartBUY[26] initiative developed blanket purchase agreements (BPAs) for commercial off the shelf software. Email-as-a-Service (EaaS) and Infrastructure as a Service (IaaS) acquisition capabilities have been delivered via enterprise-wide BPAs. The estimated value of EaaS BPAs is $2.5 billion and offers five key service offerings via four deployment models (sub-lots) through 16 industry partners for ordering activities. The estimated value of IaaS BPAs is over $76 mio and offers ordering agencies IaaS services in three key lots. BPAs are signed for up to five years and all BPA holders have agreed to standardized technical and security requirements. GSA has defined a simple procurement process to purchase EaaS/IaaS services by using BPAs[27]. For further details see Annex 3.

[24] http://www.gsa.gov
[25] https://www.fedramp.gov/
[26] http://www.gsa.gov/portal/content/105119
[27] http://www.gsa.gov/portal/mediaId/189375/fileName/IaaS_Ordering_Guide.action

5.3 Public procurement practices vs private procurement

The biggest difference between procurement practices in the public and private sector is that private sector organizations do not have to follow a strict set of rules when buying cloud services – while there may be internal checks and balances, it is not the same as spending "public" money, for which rules are inflexible. Private sector organizations will generally be outcome-oriented and can manage how they buy cloud services that best suit the situation.

PICSE has documented the five steps of a procurement process adopted by public research organizations to procure ICT services and goods (Figure 1), which mirror many of the steps that a private sector organization would take when investing in cloud services, but there would likely be little time spent on determining the most suitable procurement procedure (second step). Everything else from planning to contract and performance management would be considered.

However, the Internet2 and UK G-Cloud case studies provide some real examples of how the marketplace concept used in those case studies could be applied in the private sector – an environment with pre-tested and approved offerings, or an environment where new solutions can be tested and added to the catalog under strict and well recognized conditions. To some extent this is already happening in the ecosystems of e.g. Salesforce.com, in which apps are added to an ecosystem, which adds new services/functionalities, with a control mechanism in place to underwrite quality and reliability.

6. Best Practices

A high-level procurement process for cloud services in public research organizations has been identified in the D2.1 Research Procurement Model.

Guiding procurement principles are defined in all public research organizations and public administrations. They aim at providing overall guidance on how procurement should be conducted and values that must be maintained during the process such as transparency, fairness, efficiency, and equality. This is entrenched in internal control measures. These guiding principles usually are a fundamental part of a procurement process and are shared by public research organizations of all sizes.

From the operational standpoint, public procurement is also usually structured around a categorization of procedures based on the estimated cost of the goods or services to be acquired. The process normally foresees an increasing level of authorization and formality with the increasing monetary value of the services procured.

Public procurement generally involves competitive bidding procedures, to ensure that best quality, conditions and market prices are offered under equal and fair conditions. Nonetheless, the higher the value or risk of the operation, the more formal the control measures are for competitive bidding procedures. This ensures proper risk management and control.

Procedures reflect the guiding principles applying to the different steps throughout the procurement process. There will hence be procedures for the appropriate definition of specifications, receipt of offers, evaluation, etc., covering the complete procurement process operationalizing corresponding principles.

Guiding principles and procedures are usually supported by best practice approaches, based on benchmarking, analysis, experience and lessons learnt, which contribute to efficiency and effectiveness.

The figure below outlines the five steps that are part of the standard procurement process adopted by public research organizations to procure ICT services and goods:

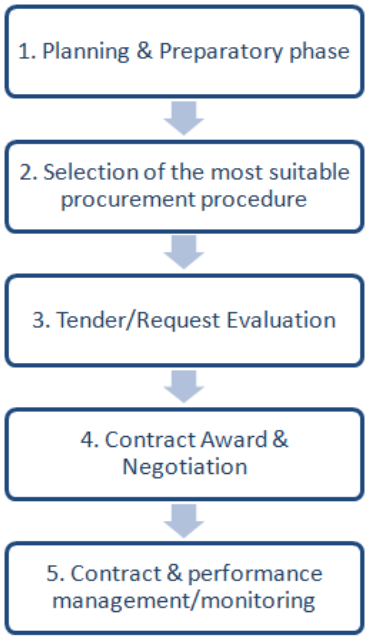

Figure 1: The five steps of a procurement process

D2.1 Research Procurement Model describes every step of the standard procurement process into detail. The model provides a set of checklists describing the procurement steps specifically for procuring cloud services. Each checklist includes a set of actions and recommendations for each procurement step related to the cloud environment. This report will propose procurement best practices to adopt, with a particular emphasis on overcoming procurement barriers from section 5.1 in the area of:

- Policy and Organisation
- Processes
- Staff
- Tools
- Cloud Service Providers

The self-assessment tool is based on the Procurement Maturity Model[28] (PMM), which was developed to assist procurement professionals in implementing procurement best practices as a means to improve organizational performance and professional skills. PICSE adapted PMM to the cloud case and used it in the PICSE Wizard as a base for assessment of procurement procedures for cloud services. The following sections include an analysis of the best practices reported in the tool:

6.1 Policy and Organisation

Identified procurement best practice related to policy and organisation:

a) Cloud Strategy in place: Documented cloud strategy, containing relevant and quality content, approved and resourced by executive management, that department staff are familiar with.

[28] http://www.stephenguth.com/procurement-best-practices-via-the-procurement-maturity-model/

b) Procurement Policy for cloud services: Documented procurement policy for cloud services, containing relevant and quality content, that department staff and internal customers are familiar with.
c) Procurement Policy aligned with a consumption based model: Documented and formalized policies to regulate the procurement of cloud services based on a consumption based model.
d) Executive support: The cloud procurement action is supported by executive management, and support is evidenced by the allocation of resources, such as budget, headcount, and training opportunities.
e) Cloud Best Practices documented: The organisation has developed and constantly updates cloud best practices that are the reference point for future cloud procurement action.

Table 1 is mapping the identified procurement best practices related to policy and organisation, identified during the analysis of case studies, interviews and literature review, with the guidelines and frameworks dealing with the procurement of cloud services.

Best practice	References/Sources
6.1.a: Cloud Strategy	EC, G-Cloud, NET+, US GSA,
6.1.b: Procurement Policy	EC, G-Cloud, NET+, US GSA,
6.1.c: Consumption based model	EC, G-Cloud, NET+, US GSA,
6.1.d: Executive support	EC, G-Cloud, NET+, US GSA,
6.1.e: Best Practices documented	EC, G-Cloud, NET+, US GSA,

Table 1: Policy and Organisation Best Practices

6.2 Processes

a) Identified procurement best practices related to processes. The Cloud business case: A cloud business case is performed at the start of the procurement action and continuously updated during the procurement and after the award of the contract. For each new procurement action, the business case is built from scratch even if the procurement is similar to the one previously performed by the organisation, because cloud markets change rapidly.
b) Technical requirements definition: Security, data protection & privacy, data and service portability, interoperability & lock-in and legacy system aspects are the core of the analysis of technical requirements and there are standard templates for the requirements collection.
c) Legal requirements definition: Data location, protection, ownership and access, privacy, confidentiality, security, breach disclosure, control of data and compliance with applicable laws and policies aspects are the core of the analysis of technical requirements and there are standard templates for the requirements collection.
d) Pre-Procurement Market engagement: Pre-Procurement market engagement enables you to consult the market and to examine alternative solutions 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 large, the procurement action may encounter some issues.
e) Cloud pilots: Even if you have experience in cloud procurement, you should not assume that the successful deployment of an application in a cloud environment is automatically a positive indication

for proceeding with deploying at large; the security and resilience requirements of each application should be examined carefully and individually and compared to the available cloud architectures and security controls. A pilot test is always recommended.

f) Joint Procurement: Joint procurement means combining the procurement actions of two or more contracting authorities. It's a way to share risks and burdens with other buyers and to increase the negotiation power towards the CSP.

g) Tender evaluation criteria: Important evaluation criteria includes pricing towards the Service Level Agreements. Termination of contract in Terms and Conditions is fundamental as well.

h) Contract negotiation: Significant amounts of negotiations are achieved by IT staff, supported by the procurement office and legal experts. Cloud negotiation standard procedures are in place or documented.

i) Cloud terms for service & performance monitoring and management: Regular monitoring & management of service & performance contract terms supported by appropriate tools.

j) Cloud contract payments, billing monitoring and management: Procedures are in place to monitor payments & billing; routinely performed.

Table 2 is mapping the identified procurement best practices related to processes, identified during the analysis of case studies, interviews and literature review, with the guidelines and frameworks dealing with procurement of cloud services.

Best practice	**References/Sources**
6.2.a: Cloud business case	G-Cloud, NET+, US GSA
6.2.b: Technical requirements definition	EC, G-Cloud, NET+, US GSA
6.2.c: Legal requirements definition	EC, G-Cloud, NET+, US GSA
6.2.d: Pre-procurement market engagement	EC, G-Cloud
6.2.e: Cloud pilots	NET+
6.2.f: Joint procurement	NET+
6.2.g: Tender evaluation criteria	G-Cloud, US GSA
6.2.h: Contract negotiation	G-Cloud, NET+
6.2.i: Cloud terms of service & performance monitoring and management	G-Cloud, US GSA
6.2.j: Cloud contract payments & billing monitoring and management	G-Cloud, US GSA

Table 2: Processes Best Practices

In addition to above best practices documented in the tool, the following practices related to processes have been identified by UK G-Cloud, NET+ and US GSA:

- Scope determination: After an organisation identifies a challenge or need, the scope of work, performance objectives and deliverables need to be defined (G-Cloud, NET+, US GSA).
- Fast-track process: For services where the standard requirements and business terms are immediately acceptable and modifications to the contract are smaller in nature, fast-track process is an efficient way to deploy services by minimising the cost/effort and increasing the time to value (NET+).

6.3 Staff

Identified procurement best practice related to staff:

a) Skills of the IT staff involved in the procurement action: IT staff involved in the procurement action undergo cloud training programmes and have cloud training objectives included as part of their annual performance plan.
b) Legal Competences related to cloud computing: A legal officer with cloud skills is present in the organisation and actively supports the cloud procurement throughout the phases (including the requirements collection). An appropriate budget is dedicated to outsourcing a legal consultant who supports the procurement team in the different phases of the cloud procurement action.
c) Procurement staff skills: Procurement officers follow a cloud training programme and have cloud training objectives included in their annual performance plan.
d) Financial staff skills: Financial officers follow a cloud training programme and have cloud training objectives included in their annual performance plan.
e) Engagement of the IT department employees: employees of the IT department are well informed about the cloud procurement action and undergo appropriate cloud training. They are aware of the ongoing changes within the organisation and they have been already interviewed to understand what role they want/can play in the new cloud scenario.
f) Cloud user engagement: Customers view procurement department staff as virtual extensions of their own staff, engaging procurement department staff in customer-specific processes, such as customer staff meetings.

Table 3 is mapping the identified procurement best practices related to staff, identified during the analysis of case studies, interviews and literature review, with the guidelines and frameworks dealing with procurement of cloud services.

Best practice	**References/Sources**
6.3.a: Skills of the IT staff involved in the procurement action	EC, NET+
6.3.b: Legal competences related to cloud computing	EC, NET+
6.3.c: Procurement staff skills	EC, NET+
6.3.d: Financial staff skills	EC, NET+
6.3.e: Engagement of the IT department	EC, NET+
6.3.f: Cloud users engagement	EC, G-Cloud, NET+

Table 3: Staff Best Practices

6.4 Tools

Identified procurement best practice related to tools:

a) Contract performance monitoring system: Automated system exists and is in use.
b) Billing monitoring system: Automated system exists and is in use.

c) Cloud procurement checklist: Cloud procurement checklist exists and is in use.
d) SLA templates: A cloud SLA template exists and the cloud procurement team is well-trained to use it.
e) Usage of cloud-based standards: The cloud procurement team has a good understanding of cloud standards. They are used to define requirements.
f) Cloud tender template: A cloud tender template exists and is in use.

Table 4 is mapping the identified procurement best practices related to tools, identified during the analysis of case studies, interviews and literature review, with the guidelines and frameworks which are dealing with the procurement of cloud services. While we were able to map the most common best practices to existing guidelines and frameworks, it seems that cloud tender templates are not adopted by the community and shows that the organisations are looking more towards the marketplace and brokerage models over performing stand-alone cloud tenders.

Best practice	References/Sources
6.4.a: Contract performance monitoring system	EC, G-Cloud, US GSA
6.4.b: Billing monitoring system	US GSA
6.4.c: Cloud procurement checklist	G-Cloud
6.4.d: SLA templates	EC, G-Cloud, NET+, US GSA
6.4.e: Usage of cloud-based standards	EC, G-Cloud, NET+, US GSA
6.4.f: Cloud tender template	

Table 4: Tools Best Practices

In addition to above best practices documented in the tool, the following practices related to tools have been identified by UK G-Cloud, NET+ and US GSA:

- Standard cloud contract: Organisation is using a standard cloud contract in the procurement process of cloud services which is considered to be “a standard specification” and pre-qualifying evaluation/review process (G-Cloud, NET+, US GSA).

6.5 Cloud Service Providers

Identified procurement best practice related to CSPs:

a) Approved CSP List: Formal, current, and documented approved CSPs list exists, and is used to ensure that 75% or more of cloud budget is spent through approved CSPs.
b) Measurements and Metrics: CSPs performance is objectively measured using predefined metrics, with performance recorded and tracked in a contract management or related system. CSPs performance measurements are mainly related to Service Level Agreements & Terms of Service.
c) Service customizability: Organisation discusses CSP product roadmap (under NDA) and determines ways in which service needs to be geared to fulfil their needs. The organisation is

able to prioritize featured requests and discusses prioritization with the CSP product team. CSP is capable to deliver a customized roadmap.

d) Contractual flexibility: Organisation negotiates business agreements, enterprise customer agreements and any associated terms of use with the CSP. Organisation's standard cloud contract templates are used for negotiation with the CSP.
e) CSP Certifications: Prospective vendors are qualified using a formal, automated process.
f) Engagement: Notification of the tender publication of official portals and appropriate advertisement on external websites. Organisation of information days & meetings open to CSPs.
g) Feedback collection: Feedback from all the bidders is collected and a procedure is in place to improve the tender/RFQ writing procedure on the basis of the feedback.

Table 5 is mapping the identified procurement best practices related to CSPs, identified during the analysis of case studies, interviews and literature review, with the guidelines and frameworks dealing with procurement of cloud services.

Best practice	References/Sources
6.4.a: Approved CSP list	G-Cloud, NET+, US GSA
6.4.b: Measurements and metrics	G-Cloud, NET+, US GSA
6.4.c: Service customizability	G-Cloud, NET+, US GSA
6.4.d: Contractual flexibility	G-Cloud, NET+, US GSA
6.4.e: CSP certifications	EC, G-Cloud, NET+, US GSA
6.4.f: Engagement	G-Cloud, NET+, US GSA
6.4.g: Feedback collection	G-Cloud, NET+, US GSA

Table 5: CSP Best Practices

In addition to above best practices documented in the tool, the following practices related to CSPs have been identified by UK G-Cloud, NET+ and US GSA.:

- Contract termination: Conditions for termination of the contract are carefully defined to avoid problems when a service is in the process of termination. Using source code escrow as part of exit strategy. (G-Cloud, NET+, US GSA).

Furthermore, according to Gartner users should negotiate conditions for termination of the contract for at least six months' notice for the provider to terminate, unless they have breached the contract.

6.6 Unaddressed barriers

Documented best practices provide ways of lowering barriers to procurement as seen in Table 6.

Procurement Barriers	Addressed by best practices
Lack of skills and competences	Staff
Organisational/cultural barriers	Policy and Organisation, Staff
Cloud business case	Processes

Legal-organisational barriers	Processes, Tools
Lack of information security assurance	Processes, Tools, CSPs
Data protection/privacy	Processes, Tools, CSPs
Data and service portability	Processes, Tools, CSPs
Interoperability	Processes, Tools, CSPs
Vendor lock-in	Processes, Tools, CSPs
Vendor liability	Processes, Tools, CSPs
Confidentiality assurance	Processes, Tools, CSPs
Performance monitoring	Processes, Tools, CSPs
Service customizability	Processes, Tools, CSPs
Contractual flexibility	Processes, Tools, CSPs

Table 6: Review of procurement barriers

However, PICSE case studies imply that not all barriers are adequately addressed by public research organisations. The adoption of cloud computing depends greatly on how the cloud can address concerns on security (confidentiality, integrity, availability), portability and interoperability. While European public research organisations do not use a systematic approach to defining security requirements during the cloud procurement process, UK G-Cloud defines essential security principles[29] to consider when evaluating cloud services. There are a number of common approaches that can be used to address several Cloud Security Principles, however the most common examples of standards and certifications for independent validation of assertions are CSA CCM[30] and ISO/IEC 27001[31] from the list of standards and definitions[32] to which the UK government guidance refers. US GSA requires CSPs to obtain a FedRAMP authorization before any ordering is permitted. Similarly, CSPs cannot be added to the Internet2 NET+ service catalogue until they fill out the CCM.

Cloud consumers need SLAs to specify the technical performance requirements fulfilled by a cloud provider. SLAs can cover terms regarding the quality of service, security and remedies for performance failures. Current practice of using SLA is limited only to performance measurement. European Commission Cloud Computing Strategy calls for the development of standardisation guidelines for cloud computing service level agreements for contracts between cloud service providers and cloud service customers. In February 2013 the European Commission DG CONNECT set up the Cloud Select Industry Group – a subgroup on Service Level Agreements (C-SIG-SLA) to work on this aspect. The C-SIG SLA subgroup, an industry group facilitated by the European Commission DG Connect, has prepared SLA standardisation guidelines[33] to provide a set of SLA standardisation guidelines for cloud service providers and professional cloud service customers, while ensuring the specific needs of the European cloud market and industry are taken into account. The document covers the following service level objectives (SLO):

- Performance SLOs
- Security SLOs

[29] https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles
[30] https://cloudsecurityalliance.org/ccm/
[31] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[32] https://www.gov.uk/government/publications/cloud-security-guidance-standards-and-definitions/cloud-security-guidance-standards-and-definitions
[33] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138

- Data management SLOs
- Personal data protection SLOs

Study report “"Standards terms and performances criteria in Service Level Agreements for cloud computing services"[34] provides model SLA clauses as a template that can be used as a starting point for the creation and assessment of SLAs for cloud computing. However, it should be integrated with other related activities such as C-SIG and other SLA-relevant outputs from EU funded projects, including Cloud4Europe, SPECS, SLA READY, A4CLOUD, and SLALOM.

Privacy is one of the main barriers and data protection/privacy provisions are usually stated within technical requirements, together with security, data portability and interoperability requirements. In order to remove barriers to cloud adoption, CSA defined baselines for compliance with data protection legislation and best practices by defining a standard format for Privacy Level Agreements[35] (PLAs) and standards, through which a cloud service provider declares the level of privacy (personal data protection and security) that it sustains for the relevant data processing, in the form of an SLA.

According to Gartner, IT procurement or sourcing managers challenged with finding sourcing options that reduce costs at tolerable risks should examine nine contractual terms to reduce risk in cloud contracts, which include uptime guarantees, SLA penalties and penalty exclusions, security, business continuity and disaster recovery, data privacy conditions, suspension of service, termination and liability.

Barriers directly impacting procurement practice in organisations are related to the use of current internal policies and procurement rules, which are not enabling easy procurement of cloud services and it is generally accepted that organisations will be able to lower those barriers through the adoption of new skills and competences by properly training all actors involved in the procurement process of cloud services. While PICSE has proposed best practices for processes and staff, European public research organisations have not developed a training programme, which would maximize the benefits of cloud computing in organisations. On the other hand, Internet2 in the USA has acknowledged such need and developed the CloudProud[36] program, which serves as a knowledge database for Internet2 members. Cloud Security Alliance (CSA) has developed a CCSK[37] certification in 2010 to address the skills gap and training for professionals in both cloud computing and security. Furthermore, the International Information System Security Certification Consortium, Inc., (ISC)²® and CSA have developed CCSP[38] certification intended for the IT staff. CCSP is most appropriate for those whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services.

While good practices for cloud procurement processes have been identified, contract termination is the process step requiring more thinking. PICSE has not noted the use of cloud escrow, which in unforeseen circumstances, ensures the organisation continued use of critical processes and data, is not commonly used.

[34] https://ec.europa.eu/digital-agenda/en/news/study-report-standards-terms-and-performances-criteria-service-level-agreements-cloud-computing
[35] https://cloudsecurityalliance.org/pla/
[36] http://www.internet2.edu/products-services/cloud-services-applications/cloudproud/
[37] https://cloudsecurityalliance.org/education/ccsk/
[38] https://www.isc2.org/ccsp/

7. Conclusion

Digital transformation is crucial to any organisation, whether public or private. It is at the very core of the digital single market to ensure Europe reaps the socio-economic benefits of new technologies. Cloud computing has the potential to reduce IT expenditure and to boost organisational agility while at the same time improving the scope for delivering flexible high-quality new services.

Barriers to the adoption of cloud services range from the shift to new procurement processes to match the cloud's on-demand model, lack of trust and security, lack of mature technical standards to complex legal terms and fear of vendor lock-in. Overcoming these barriers is key to boosting public sector productivity and efficiency, fulfilling a new set of user demand in a way that ensures secure, reliable and compliance with institutional requirements.

Finally, as identified in staff-related best practices, barriers directly impacting cloud procurement in organisations are related to **lack of training and awareness about cloud computing**. Many departments within public sector organisations do not understand what the shift to the cloud means. It is paramount for procurers to know best practices and currently there is a lack of champions showcasing their cloud success stories like the Internet2 CloudProud program. Cloud Security Alliance certifications (CCSK and CCSP) can help addressing skill gaps and provide training for professionals in both cloud computing and security.

D3.1 Procurement Barriers Report concluded that a viable marketplace and/or broker model is deemed as the best long-term solution for the scientific community and for all other target stakeholders involved in this study. Furthermore, the results of the case studies analysis show that CSPs are expected to provide::

- A catalogue of cloud service providers and related services
- More transparency in cloud pricing
- Cloud brokers at all levels (e.g. IaaS, SaaS, PaaS, skills brokerage, Information brokerage) that can efficiently speed up the cloud purchase
- Standalone tests for customers to verify the suitability of the services provided by the supplier

Cloud marketplaces such as the Helix Nebula Marketplace (HNX), UK G-Cloud, DBCE, Cloud28+ in Europe and NET+, BPA agreements in the US are offering cloud service catalogues allowing their customers to buy commoditised cloud based solutions in a transparent manner where pricing is known and brokerage services are performed by the marketplace/framework in order to ease the cloud purchase for end customers.

After analysing the procurement best practices in the 5 areas described in sections 6.1 to 6.5, which are also areas of measurement within the PICSE Wizard tool, we can conclude that marketplace/broker model seems to be the best approach to overcome the procurement barriers described in section 5.1. Best practices in the area of policy and organisation are adequately covered by most of the analysed models and the same can be said for best practices in the area of processes. Moreover, we have noted that some frameworks have additional best practices related to processes, i.e. scope determination and a fast-track process are examples of best practices identified in G-Cloud, NET+ and US GSA frameworks. However, when we look into best practices in the area of staff, we can note a lack of training activities to maximize the benefits of cloud

computing in organisations. In the area of tools, we have noted that existing guidance and frameworks are using/suggesting the identified best practices, such as contract performance monitoring system, SLA templates and usage of cloud-based standards. However, it seems that a practice for developing cloud tender templates[39] is not a practice adopted by the community and it indicates that organisations are looking more towards the marketplace and/or broker models instead of performing their own cloud tenders. We identified that G-Cloud, NET+ and US GSA frameworks adopt a practice of standard cloud contracts, which are considered to be "a standard specification" and ease cloud purchase for the organisations.

While best practices are overcoming the procurement barriers, the case studies show that not all barriers are adequately addressed by public research organisations. While cloud adoption is still inhibited to security concerns, the European research organisations do not use a **systematic approach to defining security requirements** during the cloud procurement process, however from the identified best practices we can note that CSA CCM and ISO/IEC 27001 are being most often used as baselines for definition of security requirements.

SLAs are another area where guidance and templates are being developed and various EU funded projects are delivering SLA-relevant output, including Cloud4Europe, SPECS, SLA READY, A4CLOUD, and SLALOM. Public research organisations are encouraged to **negotiate SLAs related to performance, security, data management and privacy**. Contract termination and cloud escrow are two additional areas where improvement could be made. G-Cloud, NET+ and US GSA frameworks have introduced a contract termination best practice which was also highlighted by Gartner study in 2011 [21].

[39] A practice in the area of tools, suggested in PICSE Wizard tool, as a result of literature review, case studies and interviews related to D2.1 and Procuring cloud services today reports.

8. References

[1] Kelly, A Trombley, E DeBrandt, D Veksler, C. (2015). Amazon Web Services. *10 Considerations for a Cloud Procurement.* Available: http://d0.awsstatic.com/whitepapers/10-considerations-for-a-cloud-procurement.pdf

[2] Thai, K.V. (2001). "Public Procurement Re-Examined." Journal Of Public Procurement, 9-50.

[3] Euyarra, E, Edler, J, Garcia-Estevez, J, Georghiou, L, Yeowa,J . (2014). Barriers To Innovation Through Public Procurement: A Supplier Perspective. Technovation. 34, 631-645. Available: http://www.sciencedirect.com/science/article/pii/S0166497214000388

[4] Cabinet Office. (2013). Open Standards Principles. Available: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

[5] Cabinet Office. (2012). Making Government Business More Accessible To Smes – One Year On. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61384/SME-Progress-Report-Management-Summary-One-Year-On.PDF

[6] Van Rooy, D. (2014). Cloud Computing In The Public Sector. Available: https://privacyassociation.org/media/presentations/14DPC/cloud public sector Dirk van Rooy IAPP 2014_v1.pdf

[7] Eiroforum It Working Group. (2014). E-Infrastructure For The 21st Century - One Year Later. Available: https://zenodo.org/record/13148/files/eInfra20C-plus-one.pdf

[8] Fraunhofer. (2005). Innovation And Public Procurement. Review Of Issues At Stake. Available: http://cordis.europa.eu/innovation-policy/studies/full_study.pdf

[9] Lundell, B. (2011). E-Governance In Public Sector Ict Procurement: What Is Shaping Practice In Sweden?. Available: http://www.epractice.eu/files/European Journal epractice Volume 12_6.pdf

[10] Guth, S. (2013). Procurement Maturity Model Assessment Tool V2_11. Available: http://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fstephenguth.com%2Fwp-content%2Fuploads%2F2013%2F01%2FProcurement_Maturity_Model_Assessment_Tool_V2_11.xls&e

[11] E-Irg. (2013). E-Irg White Paper 2013. Available: http://e-irg.eu/documents/10920/11274/e-irg-white-paper-2013-final.pdf/ce8a2253-aebd-4cbe-9a93-4709a1166214

[12] Technopolis group. (2013). Analysis of cloud best practices and pilots for the public sector. Available: http://ec.europa.eu/digital-agenda/en/news/analysis-cloud-best-practices-and-pilots-public-sectorhttp://ec.europa.eu/digital-agenda/en/news/analysis-cloud-best-practices-and-pilots-public-sector

[13] European Comission. (2005). Innovation and Public Procurement. Review of Issues at Stake.

[14] Cloud for Europe. (2014). D2.1. Legal implications on cloud computing.

[15] Crown Comercial Service. (2015). G-Cloud Framework. Overview and Buyers Guide.

[16] Educase, Nacubo. (2010). Shaping the Higher Education Cloud. Available: http://www.nacubo.org/Documents/BusinessPolicyAreas/ShapingTheHECloudWhitePaper.pdf

[17]DigitalStates Institute. (2014). Best practice guide for Cloud and as-a-service procurements.

Available: http://www.govtech.com/library/papers/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements.html

[18]Tufts H. S., Weiss L. M. (2013). Cloudy with a Chance of Success: Contracting for the Cloud in Government. Available: http://www.businessofgovernment.org/sites/default/files/Cloudy%20with%20a%20Chance%20of%20Success.pdf

[19]Guidelines for Public Procurement of ICT Goods and Services SMART 2011/0044. (2014). D2 – Overview of Procurement Practices. Available: http://cordis.europa.eu/fp7/ict/ssai/docs/study-action23/d2-finalreport-29feb2012.pdf

[20]Guide for the procurement of standards-based ICT Elements of Good Practice. (2012). Available: http://cordis.europa.eu/fp7/ict/ssai/docs/study-action23/d3-guidelines-finaldraft2012-03-22.pdf

[21]Gartner. (2011). Gartner Highlights IT Procurement Best Practices to Reduce Risk in Cloud Contracts. Available: http://www.gartner.com/newsroom/id/1689914

[22]Office of the Government CIO, Hong Kong. (2013). Practice Guide for Procuring Cloud Services. Available: http://www.infocloud.gov.hk/themes/ogcio/media/practiceguideindividual/Practice_Guide%282013-11%29_EN_new.pdf

[23]General Services Administration. (2016). Best Practices for Effective Cloud Computing Services Procurement within the Federal Government.

9. Annex 1: The G-Cloud framework

The G-Cloud framework is an agreement between the government and suppliers who provide cloud-based services. The framework agreement(s) allows public sector customers to buy commoditised cloud based solutions through a Framework that is compliant, regulated and refreshed allowing CCS to provide their customers with up-to-date innovative solutions. All services within these frameworks are visible within the online catalogue (Digital Marketplace) which showcases all services available through the G-Cloud framework(s). Suppliers submit their services to the G-Cloud framework when an OJEU is open. On average, an OJEU will be open for 6 weeks, every 6 to 9 months. On-boarding process is comprised of 5 mandatory steps:

1. Create, or log into, a supplier account on the Digital Marketplace.
2. Register interest in becoming a G-Cloud 7 supplier.
3. Make the supplier declaration on the Digital Marketplace. To be eligible to provide cloud services to the public sector supplier has to:
    a. agree to the framework terms
    b. provide basic supplier information
    c. answer questions to establish grounds for mandatory exclusion
    d. answer questions to establish grounds for discretionary exclusion
4. Submit service information on the Digital Marketplace, including information like a short service description, key product features and benefits, and pricing details.
5. Wait for compliance checks. CCS checks the cloud services listed on the Digital Marketplace to make it easier for buyers to find and evaluate them. The information provided is checked against the service definitions submitted for each service. CCS will evaluate submissions against a core set of criteria, as well as against a set of lot-specific criteria. The features are assured so that:
    a. the service is suitable for the framework,
    b. a consistent base level of information on the Digital Marketplace is given,
    c. buyers are aware of core service features.

Once the submission has been processed, buyers are able to find the service live on the Digital Marketplace, including comprehensive service definitions, pricing documents and supplier's terms and conditions, which enable customers to evaluate their capabilities.

The G-Cloud framework supports the "Cloud First Policy" as a way to access and use cloud based services in a flexible and agile fashion, buying only the services needed, when they are needed.

G-Cloud services are divided into 4 lots:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

- Specialist Cloud Services (SCS)[40]

The G-Cloud Buying Process

The online catalogue ensures that all service information is available up front to enable customers to evaluate services based upon best fit and/or price. This functionality facilitates a direct award. However, a customer must evaluate and identify which service best meets their requirements to enable them to direct award. The G-Cloud buying process is comprised of six important steps that must be followed to ensure that a compliant process is adhered to.

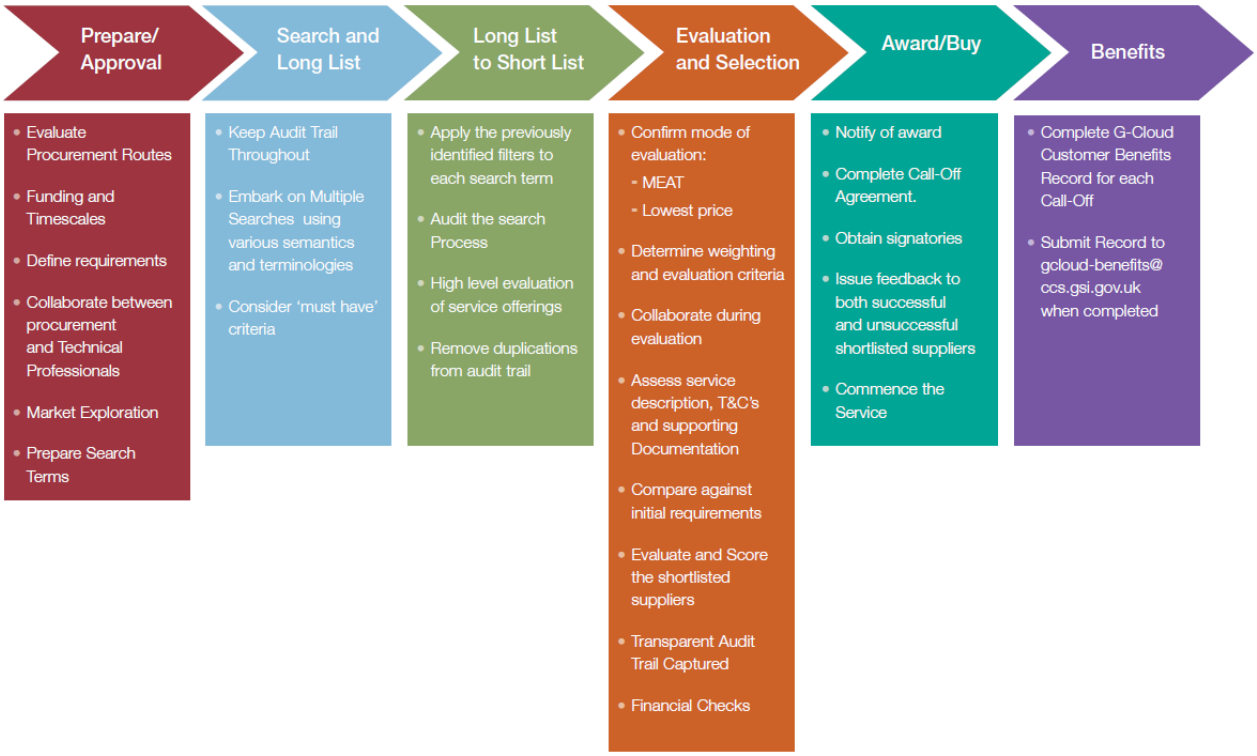

Figure 2: The G-Cloud Buying Process

The G-Cloud buying process has 6 steps:

1. Prepare: Before exploring the market place, it is essential for the customer to understand what they are looking to buy. Partnership between procurement and technical professionals is recommended to establish high-level requirements/service outputs and time-scales. Procurement expertise are essential in ensuring a compliant buying process is adhered to, whereas technical experts are required to evaluate the capabilities of the service offerings available to buy within the Digital Marketplace. Customers may wish to consider the following:
    - What funds are available for the purchase of the service
    - High level understanding of requirements (not limiting to specific details)
    - Ensure that both technical and procurement interests are covered in the requirements
    - What selection criteria will the choice be based upon? Best price or most economical advantageous tender (MEAT)
    - Is G-Cloud the correct framework for customer's need?

[40] SCS support customer transition to SaaS, PaaS and IaaS. Examples of SCS include cloud strategy, data transfer between providers or day-to-day support of cloud-based services.

Creating an extensive list of search terms will help the customer when proceeding to the long list stage. Therefore, market research would be advisable at the start of the buying process.

2. Search & long list: The purpose of formulating a long list is so that customer can refine the broad range of services available and find the service which best fits their high level requirements within the Digital Marketplace. When formulating a long list, it is important to keep an auditable trail of the search criteria as to demonstrate how and why the specific service is chosen. This audit trail needs to be done offline and away from the Digital Marketplace. It is important that customer can provide sufficient evidence to mitigate against any risk of challenge.
3. Developing long list into short list: Through applying multiple filters long list will reduce to a manageable short list of services, which can then be evaluated individually. Customer must ensure that they have captured and audited the filtering process for each catalogue search criteria. Before proceeding with shortlist evaluation, CCS would advise customer to contact the shortlisted suppliers directly in order to confirm they hold the resource capabilities to deliver to their timescales, if they were to be successful in the short list evaluation as 87% of G-Cloud suppliers are SMEs therefore their resources may be limited.
4. Evaluation and Selection: Before the customer begin the short list evaluation process it is important to understand that services are fixed at point of tender and are therefore non-negotiable. The supplier's fully comprehensive information and documentation on the Digital Marketplace is what will form part the contract and therefore needs to be evaluated accordingly. Suppliers overall service offering will include service definition, pricing document and terms and conditions. When evaluators are assessing short listed supplier service offering documents, they have to demonstrate that each service was evaluated in a fair and transparent manner. Short listed suppliers can be evaluated in two ways:
    - Most economically advantageous tender (MEAT) criteria
    - Direct award on lowest price only if they are comparable services

   The most efficient way in which to compare services is using the MEAT evaluation criteria which will allow the customer to consider best functional fit, quality and whole life cost accordingly. The overall selection process must be auditable, fair and transparent.
5. Award/Buy: Once the customer have evaluated and ascertained which service provision best meets their requirements, they are then in a position to enter into a direct award. In order to proceed, they are required to complete the appropriate Call-Off Agreement. Within the Call-Off contract, customers must clearly stipulate their service requirements up front in line with the service offering defined on the Digital Marketplace. Once complete, a copy of the Call-Off agreement must be signed by all interested parties (I.e. both the customer and supplier) before the Call-Off can commence. The maximum call of duration is 24 months and extensions are not permissible. At the end of a Call-Off, if the customer's scope has not changed and a service is still required, they must still conduct a re-evaluation of services available on the Digital Marketplace. This exercise is to ensure that the customer is still receiving the best value for money and no alternative services have been added through new iterations of the Framework. As a matter of best procurement practise, CCS would advise that customers build in a standstill period after they have notified the successful and unsuccessful shortlisted supplier. CCS would also suggest that in order to help aid the maturity of the market place customers should offer feedback relating to all of the supplier's services offerings which have been evaluated. This feedback will help suppliers to implement improvements, if they choose to retender and improve their service offering, adding value to both new and existing services, which customer in turn can then utilise in the future.
6. Benefits: CCS's remit is to work with departments and organisations across the whole of the public sector to ensure maximum value is extracted from every commercial relationship, and improve the quality of service delivery. In order to capture savings for the nation and monitor the performance

of the G-Cloud Framework(s), it is essential that customers complete the G-Cloud Customer Benefits Record form every time that they enter into a Call-Off-Agreement.

The G-Cloud Terms and Conditions

It is important for the G-Cloud customers to familiarise themselves and understand the way in which terms of the Framework function.

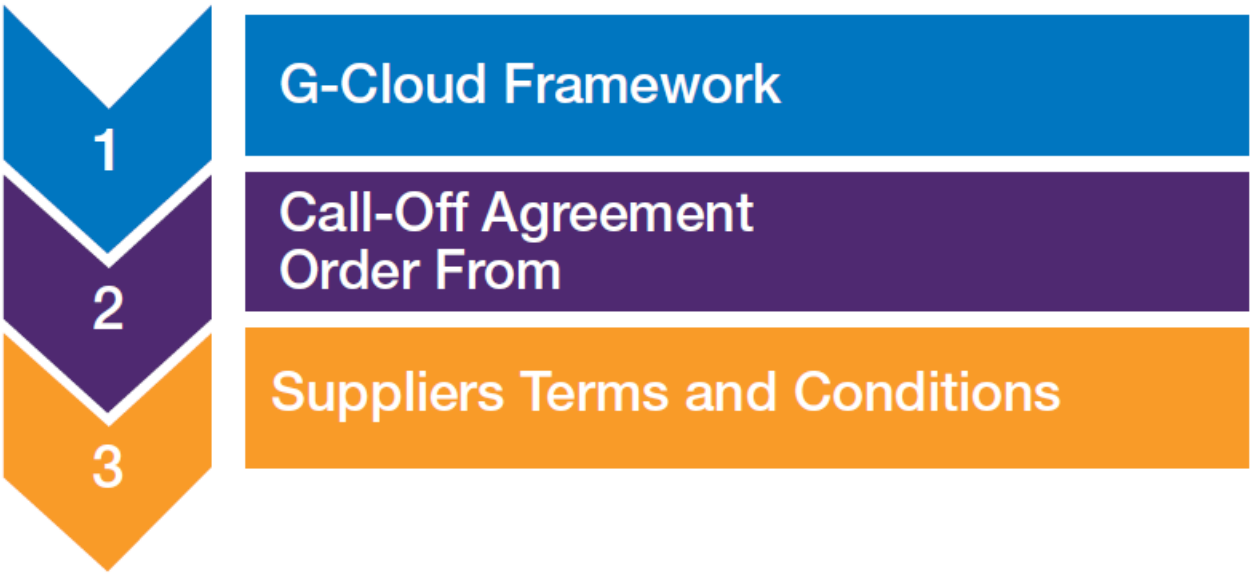

Figure 3: G-Cloud Hierarchy of Tems and Conditions Model

The G-Cloud Framework incorporates the suppliers' Terms and Conditions as it was recognised that to support the SME agenda, CCS needed to move away from the traditionally lengthy and unrealistic Terms and Conditions and embrace innovation and change. CCS, in collaboration with their legal team, was able to determine which compulsory and legally compliant terms were required for this Framework, enabling them to refine the terms and conditions and remove any unnecessary an unrealistic terms. Although the G-Cloud Framework and Call-Off Agreement Terms will take precedence, ultimately these do not determine the commercial details themselves. Instead, the suppliers terms and conditions will define the way in which the service will operate. In the case of any contradiction of terms, the Call-Off and Framework terms will take precedence. Therefore as part of short list evaluation, CCS insists that customers familiarise themselves with both the G-Cloud Framework and Call-Off terms and evaluate all short listed suppliers terms and conditions accordingly. CCS recommends that this evaluation is done by a lawyer or suitably qualified professional to assess and determine if those are in line with their organisational objectives.

10. Annex 2: Internet2 procurement approach

Internet2 is an advanced technology consortium founded by leading USA research universities, and includes more than 400 institutional members. Internet2 has created a program, called NET+, to provide new cloud-based services to higher education institutions through partnerships with commercial providers including infrastructure, platform, software, communications, and security. Shaping the Higher Education Cloud whitepaper [15] was used as genesis of NET+[41].

The core objectives of Internet2 NET+ program were to build a partnership to provide a portfolio of solutions (Figure 4) for Internet2 member organizations that are cost-effective, easy to access, simple to administer, and tailored to the unique, shared needs of the community:

- Define a new generation of value-added services
- Leverage the Internet2 R&E Network and other services such as InCommon[42]
- Drive down the costs of provisioning/consuming services
- Establish a strategic partnership with service providers (new service offerings).
- Leverage community scale for better pricing and terms
- Develop solutions that meet performance, usability, and security requirements
- Provide a single point of contracting and provisioning

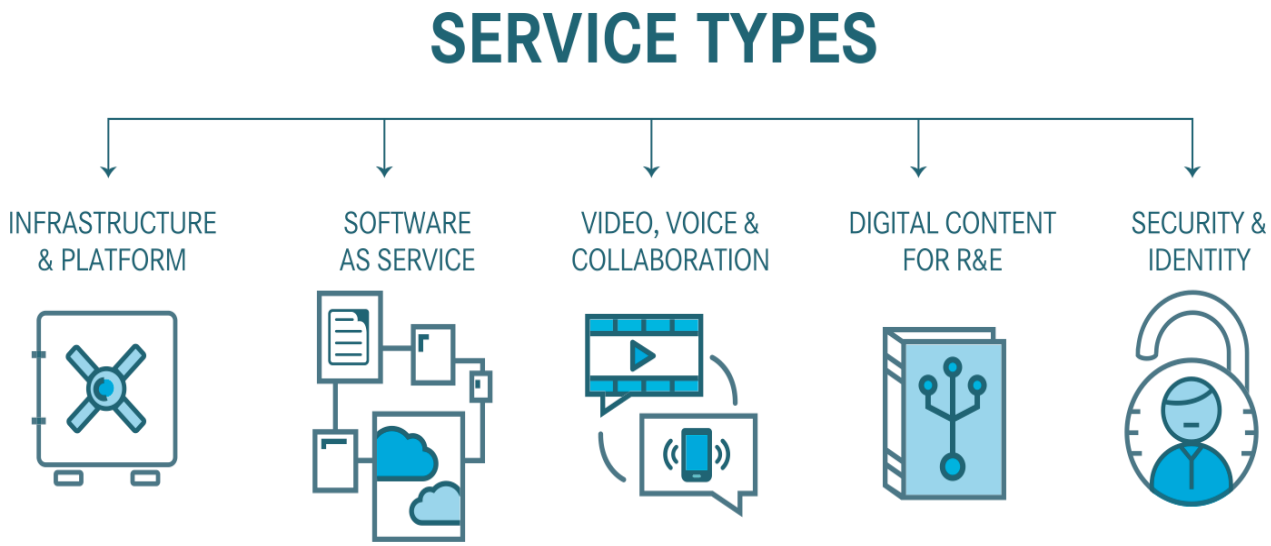

Figure 4: NET+ Portfolio Segments

Internet2 NET+ has already delivered $200M+ in estimated operating benefit for Research and Education across institutions adopting NET+ services to date. 300+ member institutions are participating in building business models, ensuring federated access, security, accessibility, performance & delivery. In average, 8 campuses are collaborating on a service validation effort before it is generally available and 3500+ research and education institutions across the US can utilise most NET+ cloud services. Currently, there are 50 services proposed for validation by Internet2 member campuses for inclusion in generally available Internet2 NET+ portfolio.

[41] http://www.internet2.edu/vision-initiatives/initiatives/internet2-netplus/

[42] InCommon provides a secure and privacy-preserving trust fabric for research and higher education, and their partners, in the US. InCommon's identity management federation serves 8 million end-users. It also operates a related assurance program, and offers certificate and multifactor authentication services.

Cloud Service Providers are eligible to offer services within NET+ only if they have a sponsor – CIO or other senior executive from a member institution; and are members of Internet2. CSPs need to adopt InCommon federation and connect their services to the R&E network. One of the requirements is to complete a customised version of Cloud Control Matrix (CCM) for Internet2 NET+. CSPs are required to commit to:

- A formal Service Validation with 5-7 member institutions
- Enterprise wide offerings and best pricing at community scale
- Establishing a service advisory board for each service offering
- Community business terms (Internet2 NET+ Business and Customer agreements)
- Support the community's security, privacy, compliance and accessibility obligations

CSPs are required to show willingness to work with the Internet2 community to customise services to meet the unique needs of education and research.

NET+ Service Lifecycle

Through a rigorous, peer-driven evaluation process, R&E institutions and cloud service providers work together to develop offerings that maximize deployment efficiencies and minimize the business and legal challenges, financial costs, and technology risks of migrating from on-campus to cloud-based solutions. Members collectively identify and vet cloud solutions that the community believes can be effective in meeting challenges, and have the potential to scale, benefiting all member institutions' teaching, learning and research needs.

NET+ services are made broadly available only after they pass this peer-driven service evaluation process. At that point, new business models, legal agreements, and the best possible pricing and terms for all are created to speed adoption and implementation. Leveraging the collective technical and functional expertise of Internet2 members, combined with the collaborative scale of the R&E community, ensures that Internet2 NET+ services are high-value, collegially vetted, ready-to-use cloud solutions, simple to access and administer, and tailored to the unique needs of R&E.

Figure 5: NET+ Service Lifecycle

NET+ Service Lifecycle has 6 service phases:

- *Inquiry*: This is where things usually start. A campus identifies a challenge; or a provider has a cloud-based service that could be used to solve a common need of the broader R&E community. These scenarios present the perfect opportunity to develop a valuable service offering.
- *Evaluation*: Internet2, service provider and university study an offering to determine whether it is suited to be an Internet2 NET+ service offering.

- *Service validation*: A sponsor and group of universities work to apply security, accessibility and performance reviews, federated authentication integration and performance optimizations. Standard legal and business agreements are then created with optimal terms.
- *Early adopter*: Universities begin using the NET+ service and continue working with Internet2 and the service provider to develop it further.
- *General availability*: The NET+ service is open to eligible universities. Quarterly Advisory Board meetings continue to inform the service development roadmap.
- *Sunset*: This phase marks the end of the lifecycle, when a service is in the process of moving out of NET+ availability, and ongoing subscriptions sunset at the end of existing terms or twelve months, whichever is later.

Research incubator is a special research phase to incubate very early stage solutions and technical concepts with a view toward possible service creation. This is used when a university is working on creating something internally, with another campus, or with a commercial partner that isn't even a product or service yet.

As seen on Figure 6, less than 50% of explored services in NET+ program reach the service validation phase. This process can take anywhere from 30 days to more than a year. Once a service reaches service validation phase, there is a 90% chance that the service will be deployed to Internet2 members. This process takes from 45 to 180 days.

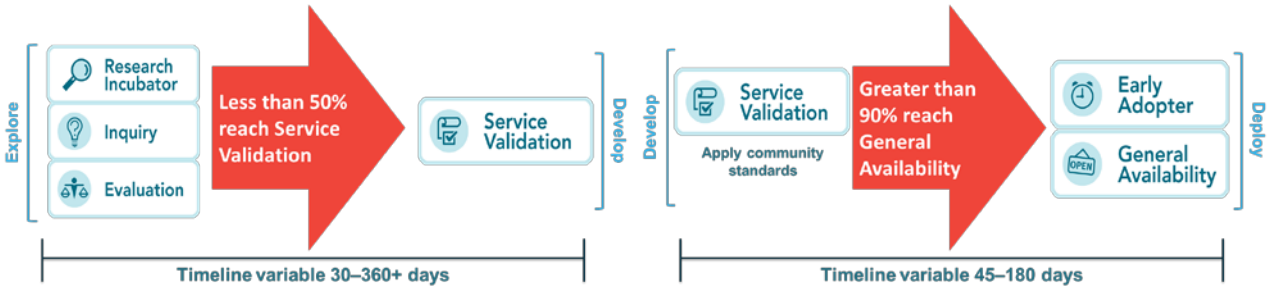

Figure 6: NET+ Service Lifecycle Timeline

We will look into the detail for the first three service phases of the NET+ service lifecycle. The Inquiry phase can go quick and includes the following steps:

- Discovery: Understanding the opportunity
- Alignment: Are the provider and community goals strategically aligned?
- Feasibility: Are the investments and mutual accommodations required likely to materialize?
- Community engagement: Membership and strategic engagement with the community

The Evaluation phase can be more time consuming and includes the following steps:

- Identifying a sponsor
- Developing a proposal
- Identifying additional Service Validation participants
- Review of requirements (networking, identity, security, business model and terms, membership in Internet2)

The Service Validation phase is an assessment of the service for inclusion in the catalogue, applying a consistent process which is available at scale to the entire higher education community. The service

validation group is led by the sponsoring institution and 5-7 campus participants which represent themselves and the community, assess the service and negotiate terms, business model and pricing for the entire R&E community. Service validation is composed from 5 components:

- Functional Assessment
  - Review current features and functionality
  - Discuss existing Service Provider product roadmap (under NDA)
  - Determine ways in which service needs to be tuned for research and education community
  - Prioritize feature requests among the participating universities in the Service Validation group and discuss prioritization with Service Provider's product team

  Process and deliverables:
  - Customized roadmap for higher education from the Service Provider
  - Feature, functionality, and bug report prioritization from the universities

- Technical Integration
  - Network: Integrate service with the Internet2 R&E network and optimize for enhanced delivery
  - Identity: Review Service Provider's identity strategy and determine InCommon integration

  Process and deliverables:
  - Service Provider and participating universities assign technical team members on networking and identity
  - Develop and review testing plans
  - Produce reference documents for service subscribers

- Security and Compliance
  - Security assessment: Customized version of the Cloud Controls Matrix (CCM) developed by the Cloud Security Alliance
  - Accessibility review and Roadmap commitment
  - Data handling: FERPA[43], HIPAA[44], privacy, data handling

  Process and deliverables:
  - Service Provider completes Cloud Controls Matrix for review by universities
  - Campus accessibility engineers review service and communicate needs to Service Provider

- Business
  - Legal: customized agreement using NET+ community contract templates.
    - MOU between Internet2 and Service Provider is signed in order to begin the Service Validation phase
    - Business Agreement between Internet2 and Service Provider is negotiated during the Service Validation phase and reviewed and approved by university counsel

[43] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/
[44] http://tn.gov/health/topic/hipaa/

- Business Model: customized approach to pricing that leverages community assets and captures aggregation to reduce costs to the Service Provider and provide savings and additional value to universities

Process and deliverables:

- Parties negotiate business agreements, enterprise customer agreements and any associated terms of use (Figure 7). All negotiations start from NET+ templates.

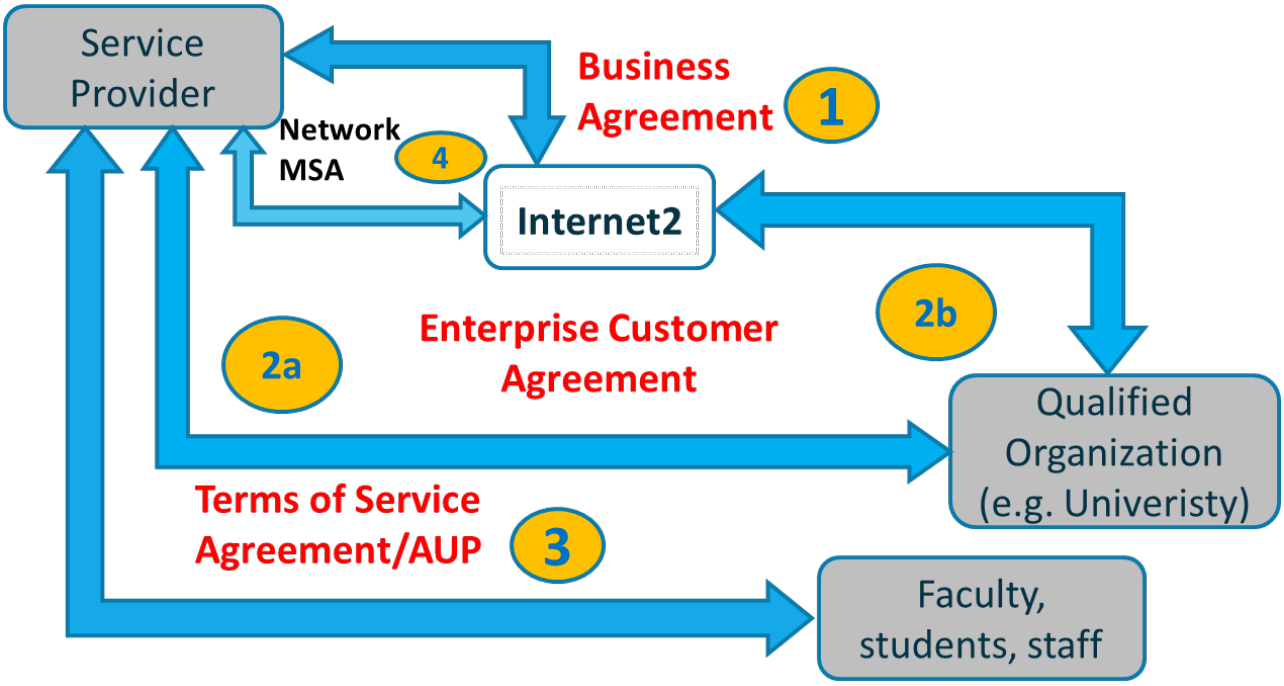

Figure 7: NET+ Contractual Relationships

- Deployment
  - Documentation: Review Service Provider's standard materials and determine the extent they need to be customized for the research and education community
  - Use cases: Universities in the Service Validation group commit to testing use cases and producing materials for the community
  - Support model: Universities provide Tier 1 support to end users, Service Provider for Tier 2/3 support via named contacts from each university

Process and deliverables:

- Service Provider and Universities work together to develop customized materials for higher education

Quick-Start Program

Internet2 has also developed a quick-start program for services where the standard requirements and business terms are immediately acceptable. Modifications to the contract template are made only to ensure appropriate representation of specific types of services. Deployment of services takes up to 6 months and in case of strong demand, the service can be put in early adoption within 60 days. The advantages of the program are:

- Provides a fast-track for on-boarding services to community requirements
- Minimizing the cost/effort required for on-boarding
- Benefit to Providers: faster time to revenue generation within the portfolio rubric and to community specifications
- Benefit to Members: faster time to value, minimum investment until scale economies and persistent interest is established, consistent adoption of community requirements

Internet2 NET+ Benefits

NET+ influences industry to develop services more useful to the Research and Education community and encourages competition among service providers on direct value of services. It encourages collaboration within the community and provides an opportunity for each member of the community to contribute to expansion of service offerings. NET+ encourages a strategic relationship between the community and service providers and provides a basis for long-term collaboration on R&D.

The main realised benefits of NET+ program are:

- Cost Avoidance
  - Lower pricing
  - Lower procurement cost/effort
- Enhanced Value
  - Favorable terms
  - Better alignment with local IT architecture
- Future Proofing (lower risk)
  - Strategic engagement with provider at community scale

NET+ mitigates the risks for the community as it:

- Reduces business risk by vetting service providers for performance, security and compliance
- Reduces contracting risk via standard (and beneficial) contract terms
- Reduces pricing risk by leveraging purchasing power of the community (including waterfall pricing)
- Ensures fair treatment in the market (no hidden clauses)
- Provides options as the number of providers in each portfolio services category increases

NET+ Agreements are being considered as an emerging standard as many universities find it valuable to consider service validation via NET+ to be “a standard specification” and pre-qualifying evaluation/review process that might allow:

- Formal procurement processes to be simplified or waived
- Not requiring formal bidding from Internet2 or NET+ validated service providers
- Eliminating the need for sole-source justification for NET+ validated service providers when only one source is available for a particular category of service
- Allowing simplified proposals from NET+ validated service providers when multiple sources are available for a particular category of service

NET+ supports procurement through community based due diligence of service providers and improves risk management by vetting service providers and providing standard and beneficial contract terms which leads to fair treatment in the market as there are no hidden clauses for “other” universities. NET+ reduces costs of administration and leverages purchasing power of the entire community. It also provides competitive options as the number of providers in each of the portfolio services category is constantly increasing.

Internet2 acknowledges that new perspectives and skills are needed to maximize the benefits of collaborative cloud environments in nearly every area of the academic institution. They have developed the CloudProud program as the trusted source where the Internet2 community turns when moving to the cloud. The key benefits of the NET+ CloudProud program are:

- Access to leading experts who share their knowledge regarding the most common barriers to moving institutions to the cloud.
- Access to the constantly growing repository of peer-to-peer cloud solution materials.
- Ability to connect and network with the Internet2 NET+ CloudProud pioneer institutions. Learn from the organizations who blazed “the cloud trail” for higher education—and took a more active role in defining the cloud service environment for our entire community.

11. Annex 3: US General Services Administration procurement approach

The US General Services Administration (GSA) serves as a centralized procurement and property management agency for the federal government. GSA focuses on implementing projects that increase efficiencies by optimizing common services and solutions across the enterprise and utilizing market innovations such as cloud computing services.

The Federal Cloud Computing Initiative (FCCI) takes a services oriented approach, whereby common infrastructure, information, and solutions can be shared/reused across the Government. The overall objective is to create a more agile Federal enterprise – where services can be reused and provisioned on demand to meet business needs. GSA is participating in the FCCI and is responsible for the coordination of GSA's activities with respect to the Initiative via its Program Management Office (CC PMO). Primary focus of the PMO is on the following activities:

- Support for cloud procurement initiatives (using vehicles such as GSA Schedule[45] or GSA Advantage[46])
- Facilitating identification of key cloud security requirements (certification, accreditation, and authorization), particularly on a government-wide basis through a FedRAMP initiative
- Promotion of current and planned cloud projects across the government
- Data center consolidation analysis, planning, and strategy support
- Development and open dissemination of relevant cloud computing information.

Cloud services are usually offered and purchased as commodities. This is a new way of buying IT services and requires careful research on both government requirements and industry capability to meet demand.

To support access to cloud-based Infrastructure as a Service (IaaS), the Cloud PMO works with the Federal Acquisition Service[47] (FAS) at GSA. FAS has primary responsibility for operating on-line acquisition services that are available for government-wide use. In May 2009, the PMO issued a Request for Information (RFI) asking the marketplace how they would address cloud computing business models, pricing, service level agreements, operational support, data management, security and standards. The responses to this RFI were incorporated into a Request for Quote (RFQ) for Infrastructure as a Service capabilities and pricing. The result was a multiple award blanket purchase agreement that agencies can use to procure cloud based web hosting, virtual machine, and storage services within a moderate security environment as defined by the Federal Information Security Act[48] (FISMA).

One of the most significant obstacles to the adoption of cloud computing is security. Agencies are concerned about the risks of housing data off-site in a cloud if FISMA security controls and accountabilities are not in place. In other words, agencies need to have valid certification and accreditation (C&A) process and a signed Authority to Operate (ATO) in place for each cloud-based product they use. While vendors are willing to meet security requirements, they would prefer not to go through the expense and effort of obtaining a C&A and ATO for each use of that product in all the federal departments and agencies. The PMO formed a security working group, initially chaired by NIST to address this problem. The group developed a process and corresponding security controls that were agreed to by multiple agencies – also known as the Federal Risk and Authorization Management Program (FedRAMP).

[45] http://www.gsa.gov/portal/content/197989
[46] http://www.gsa.gov/portal/content/104677
[47] http://www.gsa.gov/portal/content/105080
[48] http://www.dhs.gov/fisma

FedRAMP is a government-wide initiative to provide joint authorizations and continuous security monitoring services for all federal agencies with an initial focus on cloud computing. By providing a unified government-wide risk management for enterprise level IT systems, FedRAMP enables agencies to either use or leverage authorizations with:

- Vetted interagency approach
- Consistent application of Federal security requirements
- Improved community-wide risk management posture
- Increased effectiveness and management cost savings

FedRAMP allows agencies to use or leverage authorizations. Under this program, agencies are able to rely upon review security details, leverage the existing authorization, and secure agency usage of system. This greatly reduces cost, enables rapid acquisition, and reduces effort.

FedRAMP has three components:

1. Security Requirement Authorities which create government-wide baseline security requirements that are interagency developed and approved.
2. The FedRAMP Office which coordinates authorization packages, manages authorized system list, and provides continuous monitoring oversight.
3. A Joint Authorization Board which performs authorizations and on-going risk determinations to be leveraged government-wide.

SmartBUY is a Federal Strategic Sourcing Initiative (FSSI) featuring blanket purchase agreements (BPAs) for commercial off the shelf software. The FCCI partnered with GSA SmartBUY and the Department of Defense (DoD) Enterprise Software Initiative[49] (ESI) to deliver Email-as-a-Service (EaaS) and Infrastructure as a Service (IaaS) acquisition capabilities via enterprise wide BPAs. The estimated value of EaaS BPAs is $2.5 billion and offers five key service offerings via four deployment models (sub-lots) through 16 industry partners for ordering activities. The estimated value of IaaS BPAs is over $76 mio and offers ordering agencies IaaS services in three key lots. BPAs are signed for up to five years and all BPA holders have agreed to standardized technical and security requirements. Providers are required to obtain the FedRAMP ATO and are responsible for meeting the cost obligations associated with implementing, assessing, documenting and maintaining the FedRAMP control baseline.

Cloud Acquisition Lifecycle

GSA has developed the cloud acquisition lifecycle from the customer perspective and can be applied to both enterprise and project level acquisitions (Figure 8).

[49] http://www.esi.mil/

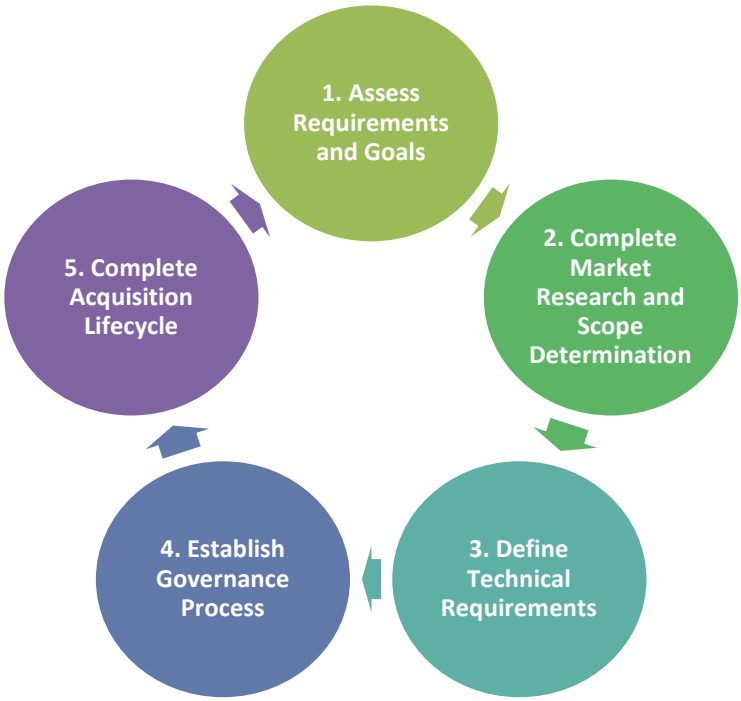

Figure 8: National Cloud Acquisition Lifecycle

1. Assess requirements and goals: A key opening step is defining the scope of the overall project. To provide a succinct, comprehensive scope and high level requirements, the buying office should always consider the following elements:
    a. Alignment to the enterprise mission
    b. Size of the anticipated effort
    c. Specific need requiring cloud services
    d. Expected results/outcomes
    e. Summary of actions to be performed by project personnel versus contractor and/or cloud service provider (CSP)
    f. Stakeholders utilizing cloud services
    g. Security, regulatory, and legal requirements
2. Complete market research and scope determination: Market research is performed to identify potential cloud solutions and vendors that may meet the enterprise or project's needs. GSA IT Schedule 70 pricing and the associated terms and conditions that are publicly available via GSA Advantage[50], and GSA e-Library[51] can be valuable aids to market research efforts beyond commercial vendor websites. The agency may also want to engage with vendors directly and early in the market research process. Speaking to vendors can help clarify scope and guide discussions to support cost benefit tradeoffs and better understand the approaches of other agencies facing similar challenges. This outreach can also help ensure vendor engagement and interest when an agency decides to issue a Request For Information (RFI). RFI's are issued by customers to gain additional information based on interest from the enterprise and can serve a useful purpose in larger procurements, providing

[50] https://www.gsaadvantage.gov/

[51] http://www.gsaelibrary.gsa.gov/

advanced advertising to vendors of the pending procurement. Some examples of RFI's include gathering additional technical specifications on cloud solutions, cloud technical implementation approaches, and contracting strategies. Depending on the jurisdiction and scope of the project there can be opportunities to leverage economies of scale through a joint procurement consolidating needs from multiple sources, either within a single agency or across entities.

3. Define technical requirements: Requirements should include consideration for normal and surge operating conditions. When specifying as-is and to-be estimates of operating conditions and capacity estimates, the following types of metrics should be considered for specification when applicable:
    a. Total utilization
    b. Average utilization
    c. Peak utilization
    d. Frequency of peak utilization occurrence
    e. Duration in time for an increase from average to peak utilization

    In the Federal sector, IT security requirements for systems are governed by the FISMA. FedRAMP provides a standardized approach to cloud security featuring a "do once and reuse many times" model to ensure FISMA compliance of cloud systems used by the government. Even if FedRAMP does not apply to a customer's particular public agency, the program publicly provides extensive security program details including guidelines, security controls, and security related standard contract clauses. In relation to SLAs, understanding and defining of the following is recommended:

    a. Terms of conditions

    b. Measures – including definitions for any measurements and related calculations

    c. Enforcement mechanisms

    Another important consideration for cloud procurement is planning from the very beginning for how the contract will terminate and services will be moved to another vendor. This may involve detailed determinations regarding, among other considerations: cessation of service, extraction of data, format(s) for the extracted data, sending the data to a new provider, and restarting key services on the new provider's platform. Building termination and migration requirements in advance will ensure adequately preparedness to transition the contract and associated services if/when necessary. Establish governance process: Successful program governance is a result of iteration with periodic performance reviews to assess and implement incremental corrections to governance processes. In cases where existing governance structures are not yet in place, process development need not be perfect from the outset but must be repeated and exercised to ensure the opportunity to refine the process exists.

4. Complete acquisition lifecycle: Once the program has established the scope, requirements, and as appropriate selected the contract vehicle, the program will develop the full solicitation. Contract templates can be very useful in these cases to ensure alignment to specific requirements of the contract vehicle and provide additional guidance. Various existing GSA contract vehicles including

Alliant[52], the EaaS BPA[53] and other agency vehicles publicly provide solicitation templates through their websites. The evaluation criteria for vendor proposals also need to be established and considered during solicitation development. Another element of solicitation development with particular cloud impact is the identification, inclusion, and integration of all relevant terms and conditions. Once the program receives the responses, it will need to evaluate each vendor's technical response against the technical evaluation criteria previously developed. This source selection process needs to rate each proposal fairly to determine the best proposal submission. Once the evaluation and scoring is complete, the award is made and officially announced. BPAs have predefined reporting requirements. Surveillance and monitoring, performance assessment and timely invoice processing are standard administration practices used.

[52] http://www.gsa.gov/alliant

[53] http://www.gsa.gov/eaas