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: MS3 Best practice interim release

Submission Due Date: M12 (October 2015)

Actual Submission Date: 29.10.2015

Work Package: WP3

Responsible Partner: CSA

Distribution: Public

Nature: Report

Abstract: This report will include: • a collection of procurement good 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 (e.g. USA). • a comparison between procurement practices in the public and private sector • a description of how current good 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:	MS3
Deliverable title:	Procurement Best Practice interim release
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:	V0.7

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

Table of Contents

List of Figures

1. Introduction

With the advent of cloud computing, the delivery of Information and Communications Technology (ICT) services is going through a fundamental change. In 2020 IDC's baseline scenario shows the total cloud market to be worth some €44.8bn (€32.7bn for the Public Cloud and €12.06bn for the private) [1].

Growing demand for computing power from public research organizations has resulted in initiatives such as Helix Nebula[2], a partnership between big science and big business in Europe that is charting the course towards the sustainable provision of cloud computing in public research organizations. However, cloud computing as a type of ICT is disrupting the traditional notions of information technology. Procurement processes and policies in many research organizations are inadequately addressing the on-demand model of cloud computing, introducing barriers to procurement of cloud services.

This report identifies and documents best practices for procuring cloud services in the public research organisations. While the report focuses on research sector, we considered also the procurement practices of cloud services in the public administration. This is because public administrations and agencies are a large consumer of ICT, and via their procurement power can have significant influence on innovation and competitiveness in the ICT market. The procurement of ICT by public organisations also represents a significant source of expenditure in 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 making the best use of public funds.

The work done in this report builds on a number of sources: 1) the analysis of good practices in public research organisations and public sector, performed in D2.1 Research Procurement Model[3], 2) the analysis of procurement barriers identified in D3.1 Procurement Barriers Report[4], 3) on the insight and knowledge gained from the Helix Nebula flagships, 4) the information obtained from the Cloud for Europe project, 5) the Internet 2 / Net+ Initiative[5], 6) the USA General Service Administration (GSA) and FCCI, FedRAMP[6], BuySMART[7] initiatives, 7) the information provided by Industry Associations (e.g. DigitalEurope), and 8) 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 types of barrier identified in D3.1. This report also highlights potential challenges likely to be faced in the future. This report is proposing a procurement best practice suitable for the European Scientific Community in the light of those challenges.

The objectives of the report are to provide mechanisms for lowering barriers to the procurement of cloud services, as described in the report "D3.1 Procurement Barriers Report", to understand how the best

[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] http:// http://www.helix-nebula.eu/
[3] http://www.picse.eu/publications/deliverables/d-21-research-procurement-model
[4] http://www.picse.eu/publications/deliverables/d31-procurement-barriers-report
[5] http://www.internet2.edu/vision-initiatives/initiatives/internet2-netplus/
[6] http://www.gsa.gov/portal/category/102375
[7] http://www.gsa.gov/portal/content/105119

practices identified in this report support the work done by the PICSE consortium in the report D2.1 Research Procurement Model and finally to provide input to the PICSE Procurement Roadmap (D 2.3).

1.1 Structure of the Report

This report is set out in the following sections:

Section 2 – Scope and Objectives of the report

Section 3 – Target Audience

Section 4 – PICSE Task Force

Section 5 – Methodology and Approach

Section 6 – Approach and barriers to procurement of cloud services

Section 7 – Best Practices

2. Scope and Objectives

The initial scope of this report was cloud computing procurement best practices in the public research organisations. Since there are commonalities between procurement practice used by public research organisations and public administration, it was decided to extend the scope of this work 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[8], a web-based application that describes the procurement models from 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 give procurers confidence that they have met their compliance obligations and that they are getting an appropriate solution to meet their needs.

[8] 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 into the cloud and so are the data they handle and work with. This means that many of them are either procuring, planning to procure or building cloud services with a view to forming a hybrid cloud.

This report will help public research organisations, public administration and, eventually, the private sector 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 are among the beneficiaries of this report as explained below.

3.1.1 Procurement Initiator

The individual nominated by the management, usually with a technical background that 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.

3.1.2 Technical Officer (IT manager)

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

3.1.3 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.

3.1.4 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.

3.1.5 Cloud Service Provider (CSP)

The Cloud Service Provider (CSP) is the ICT vendor.

4. Methodology and Approach

This study is predominantly built on qualitative methodological instruments, namely literature research and targeted interviews.

The literature review was restricted to English language documents, with a focus on the timeframe 2011-2015, since Cloud Computing is relatively recent and has evolved at a rapid pace.

An extensive research 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 the procurement best practices.

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

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 Procuring cloud services today report[9]
3. Targeted interviews with Internet2 and USA GSA
4. Consultation with the PICSE Task Force members
5. Organisations of targeted workshops & participation to target events to discuss good practices
6. Presentation of results

[9] 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

5.1 Procurement Barriers

The adoption of cloud computing services is inhibited, between other factors, by barriers related to procurement, perceived trustworthiness, technical standards and legal terms of reference, risk of vendor lock-in, etc. Potential cloud customers in the research area, across public and private sectors are not always ready for cloud services as they are 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 list of main barriers in a procurement process of cloud services has been put together from the outcomes of D2.1 Research Procurement Model and D3.1 Procurement Barriers Report. Barriers can be summarized as follows:

- Lack of skills and competences: All actors involved in the procurement process should have a clear 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 already at the time of procurement, as they may incur additional costs.
- Cloud business case: Financial issues associated with the new way of cost evaluation in moving to the cloud 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 costs savings and efficiency gains should be considered.
- 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 customizability and contractual flexibility: those are two important barriers noted by the demand side. 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 missing.

5.2 Existing Procurement approaches

PICSE has consulted with the various public research organisations and public administration (both European and US) in order to capture the current state and approach to procurement of cloud services. From this consultation phase a set of relevant good practices were identified.

- ***European intergovernmental organisations*** (e.g. CERN[10], ECMWF[11], EMBL[12], and ESA[13]) 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 belonging to the member states funding the organization can be considered eligible), size (SMEs are often considered as 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.

The PICSE Procuring cloud services today[14] report describes the experience of ten public sector organisations across Europe who 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

[10] home.web.cern.ch/
[11] http://www.ecmwf.int/
[12] http://www.embl.de/
[13] http://www.esa.int/ESA
[14] http://picse.eu/sites/default/files/Procuring%20cloud%20services%20today_22072015.pdf

approaches looking into the US procurement approaches of Internet 2 Net+ initiative and the USA General Service Administration.

5.2.1 Internet2

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+[15].

The core objectives of Internet2 NET+ program were to build a partnership to provide a portfolio of solutions (Figure 1) 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[16]
- 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

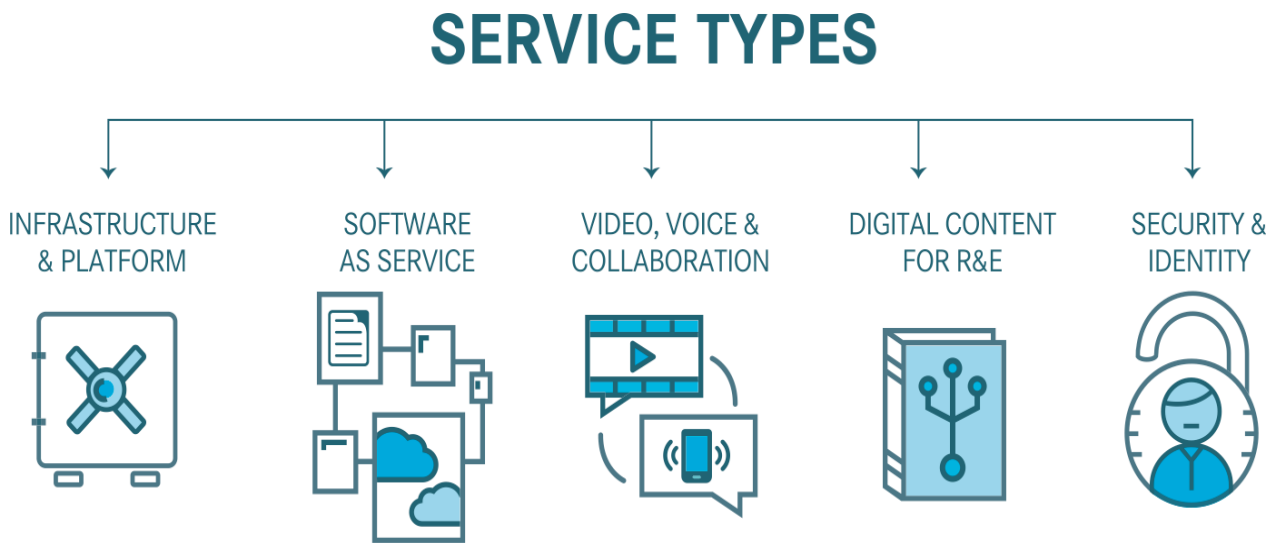

Figure 1: NET+ Portfolio Segments

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

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

[16] 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.

proposed for validation by Internet2 member campuses for inclusion in generally available Internet2 NET+ portfolio.

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[17] 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 2: NET+ Service Lifecycle

NET+ Service Lifecycle has 6 service phases:

[17] https://cloudsecurityalliance.org/ccm/

- *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 3, 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.

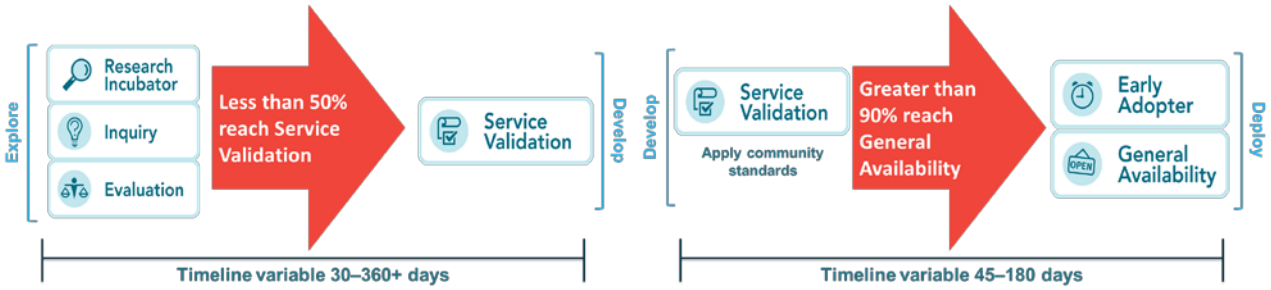

Figure 3: NET+ Service Lifecycle Timeline

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[18], HIPAA[19], 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.

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

- 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

- 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 4). All negotiations start from NET+ templates.

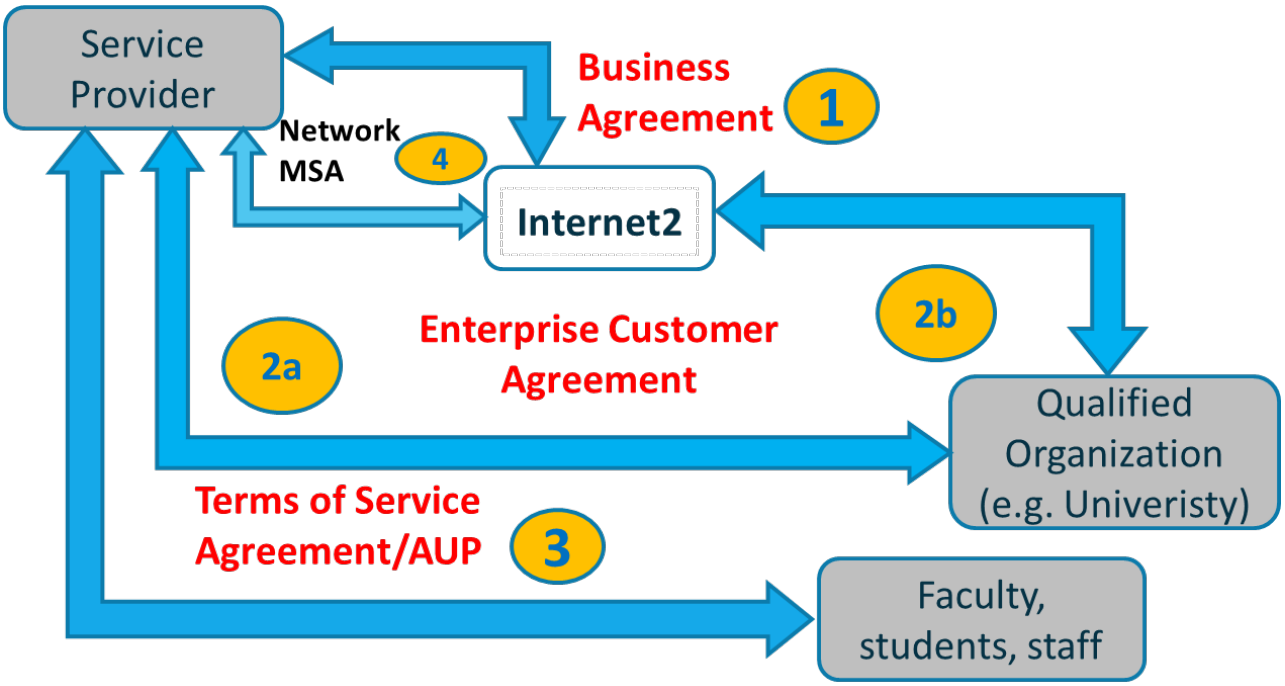

Figure 4: NET+ Contractual Relationships

- 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[20] 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.

5.2.2 US General Services Administration

The US General Services Administration[21] (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[22] or GSA Advantage[23])
- Facilitating identification of key cloud security requirements (certification, accreditation, and authorization), particularly on a government-wide basis through a FedRAMP[24] 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[25] (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)

[20] http://www.internet2.edu/products-services/cloud-services-applications/cloudproud/
[21] http://www.gsa.gov
[22] http://www.gsa.gov/portal/content/197989
[23] http://www.gsa.gov/portal/content/104677
[24] https://www.fedramp.gov/
[25] http://www.gsa.gov/portal/content/105080

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[26] (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).

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[27] 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[28] (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

[26] http://www.dhs.gov/fisma
[27] http://www.gsa.gov/portal/content/105119
[28] http://www.esi.mil/

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.

Steps to order from EaaS/IaaS BPAs

GSA has defined seven simple steps for procurement of EaaS/IaaS services by using BPAs[29]:

1. Scope determination: This is where it is determined if the requirements are within scope of the BPAs. BPA scope, terms and conditions and other relevant information such as SLAs, Security are publicly available[30].
2. Prepare Statement of Work (SOW) and/or Statement of Objectives (SOO)[31]: This is where scope of work, performance objectives, technical requirements and deliverables are defined.
3. Prepare the Request for Quote (RFQ): Following usual procurement procedures and processes for preparing an RFQ for IT products and services. The RFQ topics such as order value and funding restrictions, SLAs (performance measurements) and evaluation factors are considered.
4. Issue the RFQ: Ordering agencies must issue their RFQs to all BPA holders offering the requested services. BPA vendors must obtain a FedRAMP authorization before any ordering on the BPA is permitted.
5. Evaluate: Evaluation of all responses received using selected evaluation approach, e.g. “best value”. Ordering agencies determine their own evaluation criteria.
6. Award: Placing of the order and document the BPA holder receiving the order and all BPA holders considered, description of what was purchased and agreed upon pricing, used evaluation methodology, rationale for any tradeoffs, determination of price reasonableness and rationale for using other than a performance-based order.
7. Task Order Administration: BPAs have predefined reporting requirements. Surveillance and monitoring, performance assessment and timely invoice processing are standard administration practices used.

[29] http://www.gsa.gov/portal/mediaId/189375/fileName/IaaS_Ordering_Guide.action
[30] http://www.gsa.gov/iaas, http://www.gsa.gov/eaas
[31] http://www.gsa.gov/portal/content/133795

6. Best Practices

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

Guiding procurement principles are defined in all public research organizations and public administrations. They are aimed 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 are usually 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 service 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 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:

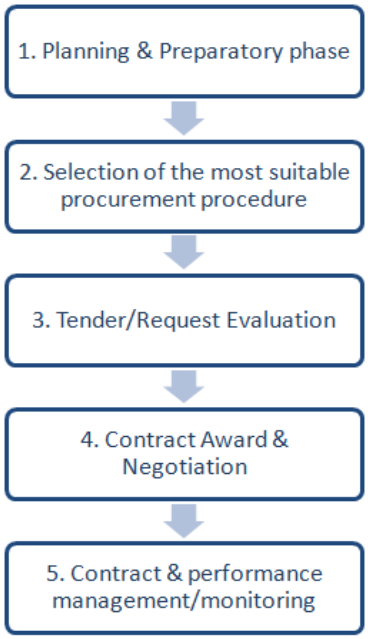

Figure 5: The five steps of a procurement process

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 6.2 in the area of:

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

The self-assessment tool is based on the Procurement Maturity Model[32] (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.

[32] 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 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.

6.2 Processes

Identified procurement best practice related to processes:

- Scope determination: After an organisation identifies a challenge or need, the scope of work, performance objectives and deliverables need to be defined.
- Cloud business case: A cloud business case is performed at the beginning 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 done from scratch even if the procurement is similar to the previously performed by the organisation because the cloud market changes rapidly.
- Technical requirements definition: Security, data protection & privacy, data and service portability, interoperability & lock-in and legacy systems aspects are the core of the analysis of technical requirements and there are standard templates for the requirements collection.
- 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.
- 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 great, the procurement action may encounter some issues.
- 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 many other deployments; 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.
- 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 increase the negotiation power towards the CSP.
- Tender evaluation criteria: Important evaluation criteria include the pricing towards the Service Level Agreements. Termination of contract in Terms and Conditions is fundamental as well.
- 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.
- Contract negotiation: Significant amount of negotiations are conducted by the IT staff, supported by the procurement office and the legal expert and cloud-negotiation standard procedure are in place or documented.

- Cloud terms of service & performance monitoring and management: Regular monitoring & management of contract terms of service & performance supported by appropriate tools.
- Cloud contract payments & billing monitoring and management: Procedures are in place to monitor payments & billing; routinely performed.
- 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.

6.3 Staff

Identified procurement best practice related to staff:

- Skills of the IT staff involved in the procurement action: IT staff involved in the procurement action follows a cloud training programme and have cloud training objectives included in the annual performance plan.
- Legal Competences related to cloud computing: A legal officer with cloud skills is present in the organisation and actively supports the cloud procurement in all the phases (including the requirements collection). An appropriate budget is dedicated to outsource a legal consultant that supports the procurement team in the different phases of the cloud procurement action.
- Procurement staff skills: Procurement officers follow a cloud training programme and have cloud training objectives included in the annual performance plan.
- Financial staff skills: Financial officers follow a cloud training programme and have cloud training objectives included in the annual performance plan.
- Engagement of the IT department employees: The employees of the IT department are well informed about the cloud procurement action and they followed appropriate cloud training. They are aware of the changes that the organisation is doing and they have been already interviewed to understand what role they want/can cover in the new cloud scenario.
- Cloud users 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.

6.4 Tools

Identified procurement best practice related to tools:

- Contract performance monitoring system: Automated system exists and is in use.
- Billing monitoring system: Automated system exists and is in use.
- Cloud procurement checklist: Cloud procurement checklist exists and is in use.
- SLA templates: A cloud SLA template exists and the cloud procurement team is well-trained on its use.
- Usage of cloud-based standards: The cloud procurement team has a good understanding of cloud standards. They are used to define requirements.
- Cloud tender template: A cloud tender template exists and is in use.

6.5 Cloud Service Providers

Identified procurement best practice related to CSPs:

- Approved CSP List: Formal, current, and documented approved CSPs list exists, and is used to ensure that 75% or greater of cloud spend is through approved CSPs.

- 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.
- Service customizability: Organisation discusses CSP product roadmap (under NDA) and determines ways in which service needs to be tuned for their needs. The organisation is able to prioritize features requests and discuss prioritization with the CSP product team. CSP is capable to deliver a customized roadmap.
- 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.
- CSP Certifications: Prospective vendors are qualified using a formal, automated process.
- Engagement: Notification of the tender publication of official portals and appropriate advertisement on external websites. Organisation of information days & meetings open to CSPs.
- Feedback collection: Feedback from all the bidders are collected and a procedure is in place to improve the tender/RFQ writing procedure on the basis of the feedback.
- Contract termination: Conditions for termination of the contract are carefully defined to avoid problems when a service is in the process of termination.

7. 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 Commission. (2005). Innovation and Public Procurement. Review of Issues at Stake.

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

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