Séptima Conferencia de Directores de Tecnología de Información, TICAL 2017
Gestión de las TICs para la Investigación y la Colaboración, San José, del 3 al 5 de julio de 2017

Advanced brokering of hybrid clouds to institutions in the Netherlands

Michel Wets[1], Harold Teunissen[2]

Surfnet, Netherlands

michel.wets@surfnet.nl

Presentation summary. Education and research institution increasingly use public cloud services as part of their internal IT and in education. Getting these services in line with the R&E requirements on e.g. privacy and security is not easy. On request of six universities of applied science, SURFnet create a hybrid cloud service which gives institutions access to a wide range of IaaS and PaaS services from both SURFnet and a wide range of European and US public cloud providers. These services have subsequently been made available to all Dutch institutions connected to SURFnet. SURFnet participated in a joint public tender with 35 other European NRENs for the public providers. Institutions can consume these services without having to run a tender themselves. IT departments, teachers and researchers can transparently see the capabilities and associated costs and choose which provider to use for which specific applications. The cloud management portal ,through which all these services are managed and provisioned, serves as a single control plane. It standardizes (and automates) tasks and gives institutions the ability to control (and limit) costs.

During this presentation, we will:

- explain the collaboration between SURFnet and Dutch institutions on cloud services;
- describe the process from initial requests to the service created;
- report on the joint European NREN IaaS tender through GEANT
- present the SURFcumulus hybrid IaaS services

---

1 **Michel Wets**: heads the Cloud team within SURFnet's Enriched Technologies department and is as Product Manager responsible for the SURFcumulus service. Michel joined SURFnet in 2011 and has been working in the IT sector for 25 years in a variety of roles, ranging from hands on IT, project management, architecture, procurement and account management to product management.

2 **Harold Teunissen**: As head of the Enriched Technology department I am responsible for the full product lifecycle of cloud and education services. Also I am leading the "incubator" initiative at SURFnet. I am leading the current Community Cloud efforts at SURFnet creating a broad set of cloud services ranging from a hybrid IaaS service SURFcumulus (VMware, Azure, AWS), to end-user filesharing services like SURFdrive and SURFfilesender.

- explain how it meets the needs of Dutch Institutions on legal, privacy, security and predictability of costs

1. SURF cooperative

The SURF cooperative serves as a joint platform where Dutch research universities, universities of applied sciences, university medical centers, research institutions and senior secondary vocational education institutions work together to develop ICT innovations. This collaboration extends to various levels: administrative, policy and operational.

1.1. Structure

SURF U.A. Cooperative is a cooperative association with excluded liability. The SURF cooperative consists of the cooperative office (SURF office) and three operating companies: SURFmarket, SURFnet and SURFsara. SURFnet is the Dutch NREN servicing 180 (middle and higher) education and research institutions with 500.000 end-users in The Netherlands.

1.2. Member-owned

The members become co-owners of SURF by signing a membership statement. Education and research institutions that have signed this statement are under obligation to purchase services provided as a part of SURF's core package (a process referred to as insourcing). This obligation only applies if the institution in question is in need of such services. The insourcing agreements exclusively apply to institutions that hold membership of the cooperative.

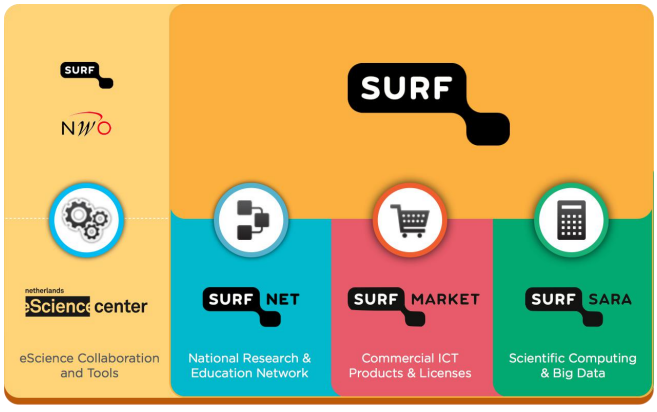

Fig.1, the SURF organization.

SURFnet operates over 9.000 km of dark fiber within the Netherlands to connect its institutions with speeds up to 100 Gbps, using light paths, IPv6 and IPv4.

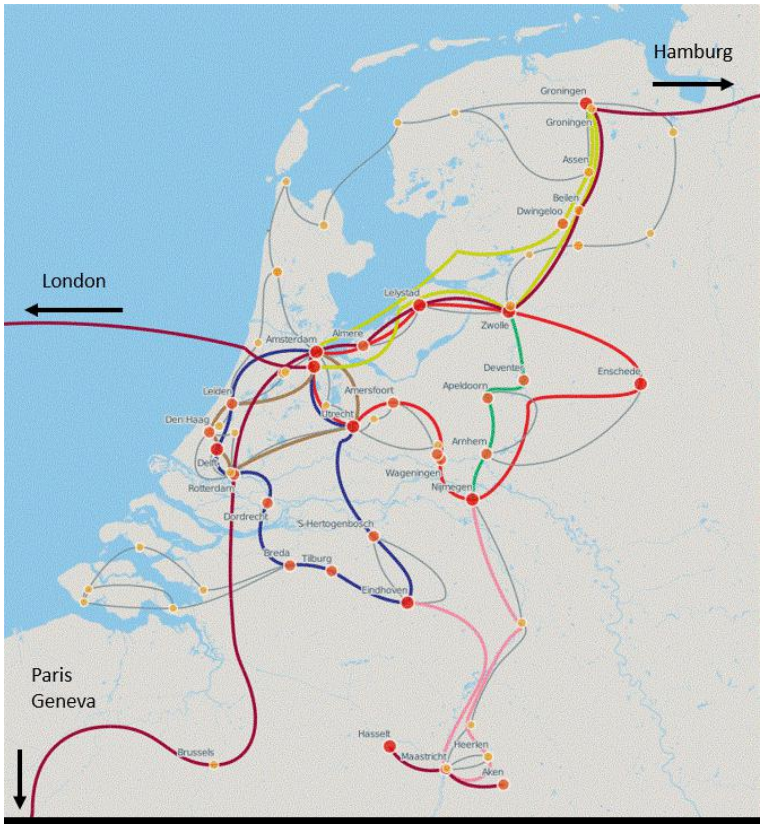

Fig.2, the SURFnet footprint and service delivery

1.3. The changing role of the NREN

Traditionally, NRENs have been primarily network orientated creating innovative services for their institutions (technology push). Increasingly, institutions in the Netherlands have been looking at SURFnet to procure and deliver complex commodity services for which they see a uniform need among institutions. This lead to the creation of a SURF cloud approach in which:

- A limited number of institutions contribute money and resources and create a uniform set of requirements
- SURF uses desk- and market research to investigate the viability of the service

- SURF creates a Service Proposition including a cost calculation aiming to break even over a three year period.
- Institutions accept the Service Proposition and sign up for the initial three years
- SURF creates the Service
- Other institutions can join the service as is.
- All participating institutions are involved in the governance and roadmap of the service.

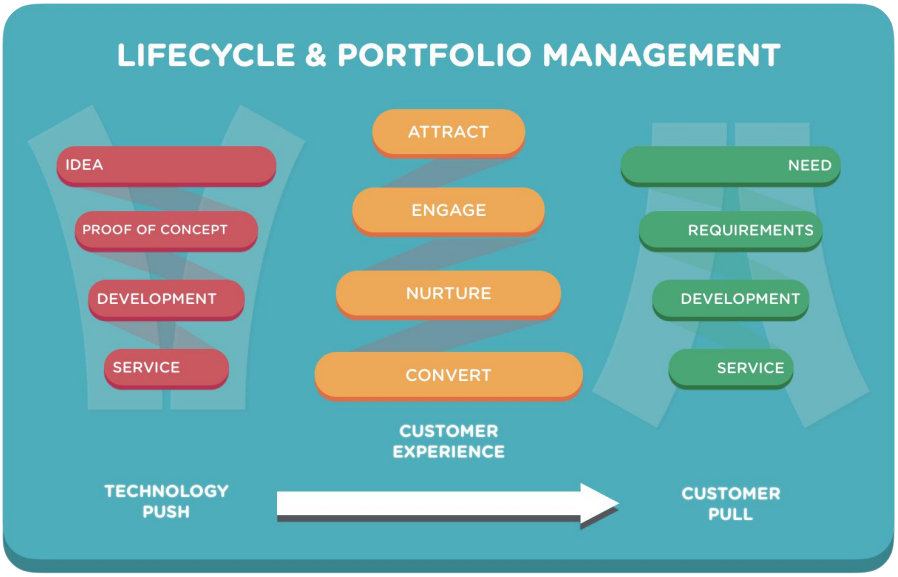

Fig. 3: evolving LCPM within SURFnet

1.4. From Operation to Directing

The use of the cloud requires a different set of competences of an ICT-organization from when it provisions and manages its own infrastructure. When an ICT organization increases the use of more off-site services, an organizational transition to a Director approach becomes needed. One of the most important roles of such a Director organization is the reconciliation between the demand of customers and supply from the market.

Because the Cloud market is in continuous development, keeping up is not a trivial task for an individual SURF-member. In the community cloud variant, suppliers can be managed on market conformity of service delivery. SURF can play the role as Supply Manager by aggregating the demand from its members, matching it with supply from the market.

1.5. SURFnet as outsourcing organization

SURF is increasingly developing towards becoming a vendor/broker of different ICT services. There are great similarities in the activities carried out for all those services. In addition, uniformity in customer contact is very much desired by institutions. For both SURFwireless (wifi as a service) and SURFcumulus Managed a Director-group has been created. For SURFcumulus Managed, the essence of Directing is having control on the orchestration, delivery and maintenance processes with the aim of optimizing customer satisfaction.

2. SURFcumulus service

2.1. SURFcumulus Basic and Managed architecture

SURFcumulus is the hybrid Infrastructure-as-a-service-service (IaaS) SURFnet. It provides institutions with a wide range of IaaS services in which SURF manages the hardware, network and virtualization while the institutions manages the operating system, the data and the application. It allows you to move VMs (virtual machines) without running a procurement against the right conditions of use and guarantees to public IaaS providers.

2.2. SURFcumulus is available in two versions: Basic and Managed

Both use the same core services:

- Services were procured through a European tender. Institutions can use these services without having to run lengthy procurement processes themselves;
- SURF handles the purchase and care of the contract;
- Privacy: all public providers meet the standards of the SURF Framework of Legal Standards for (Cloud) Services[3];
- SURF provides transparency on the data classification which the public providers have been proven to be able to support. SURF checks during the contract period that the provider continues to meet its audit obligations;
- SURF provides the invoicing towards the institutions;
- All providers are connected directly to the SURFnet network so they can be used quickly and safely.

3 https://www.surf.nl/en/knowledge-base/2013/surf-framework-of-legal-standards-for-cloud-services.html

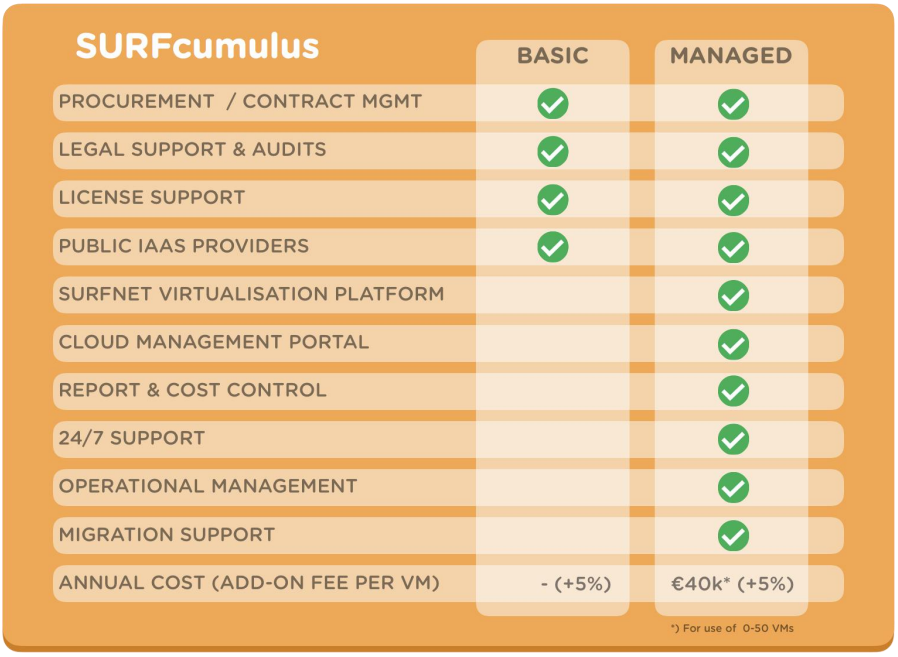

Fig.4: SURFcumulus Basic and Managed side by side

2.3. The public providers

In 2017, Microsoft Azure, Amazon AWS, Dimension Data and Interoute will join the current public IaaS providers KPN and Vancis to create a broad set of IaaS services. Services of CloudSigma can be added at a later time if their services are of additional value.

2.4. SURFcumulus Managed added value

SURFcumulus Managed allows institutions to take the driver seat while SURFnet manages the IaaS services. The institution can concentrate its ICT resources on the internal organization.

The advantages of SURFcumulus Managed:

- Supporting the institution cloud transition process through:
- Optional usage to the, on VMware based, SURFnet Virtualization Platform (SVP)
- Manage all your cloud resources through a central Cloud Management platform (CMP)

- Business case tool, allowing a TCO comparison between the cloud and your own infrastructure costs
- Actively aiding cloud strategy creation and supporting migrations
- Independent advice
- 24/7 support
- Facilitate supplier trainings
- Active vender management
- Participation of all institutions using SURFcumulus Managed in the governance workgroup, controlling the further development of the service (roadmap items and prioritization)
- Access to SURFnet Cloud expertise center:
- Promoting and facilitating collaboration between institutions
- White papers, PoC templates and use case sharing
- Independent workshops on tactical and operational level

The essence of SURFcumulus Managed is that it enables institutions to use a broad spectrum of IaaS providers, with the right conditions, while SURFnet provides the operational management of the platforms. This allows institutions to use a multi-cloud strategy where the specific requirements of a workload decide on the best cloud provider to use. The institution can concentrate on managing and monitoring the usage of the resources. SURFnet acts as broker and director of the IaaS service delivery, manages and monitors the complete service delivery chain and manages the providers and is the single point of contact for the institutions.

3. Key components of SURFcumulus Managed

3.1. SURFnet Virtualization Platform (SVP)

This, on VMware based platform allows institutions with a safe haven, allowing institutions a place to host VMs when public IaaS providers are not (yet) able to meet specific requirements.

3.2. Cloud Management Platform (CMP)

The CMP is the single glass of pane functioning as a self-service portal allowing institutions to manage their IaaS resources over all providers in a uniform way. This lowers risks as engineers, teachers and students can choose from a limited set of options, avoiding situations where they chose the wrong option (e.g. too costly or an inappropriate datacenter). The CMP runs within a SURFnet datacenter and is accessible through an, on SAML2 based, federated authentication mechanism used by all Dutch institutions.

The Role Based Access Control allows institutions to create cost based groups and control access and rights within their organization while centralized logging allows reporting on changes including who provisioned which VM at which moment.

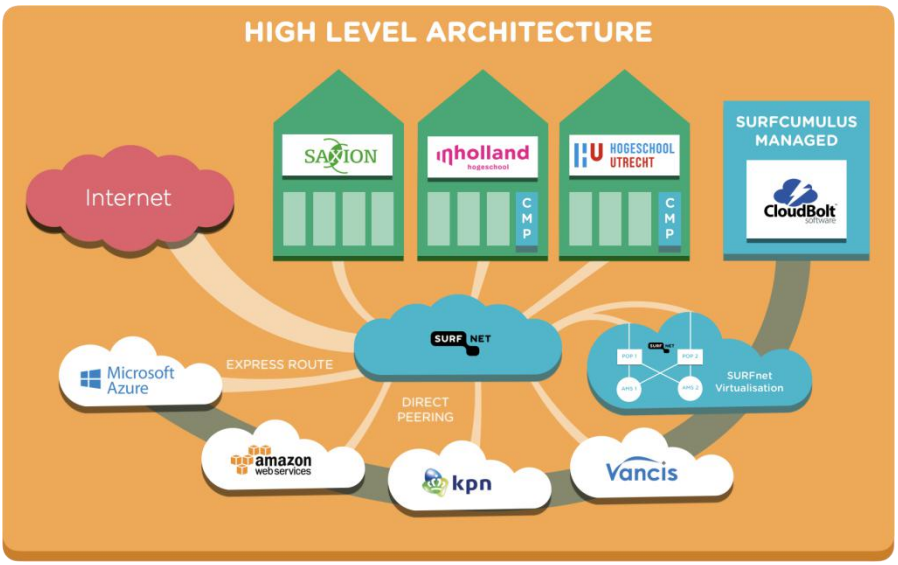

Fig. 5: High level architecture SURFcumulus

3.3. SURFnet cloud Director group.

This group of five SURF internal employees ensure that the SURFcumulus Managed service keeps meeting the key requirements of institutions, monitor the public provider performances and act as an escalation team. They fulfill the following roles:

- Product Manager: responsible for the SURFcumulus service including Profit and Loss.
- Service Delivery Manager(s): responsible for the contact with the institutions, helping them in their cloud strategy, roadmaps, proof of concept, migrations and responsible for customer satisfaction.
- Manager Operation: responsible for the CMP, SVP and managing the service delivery of the public IaaS providers.
- Contract Manager: responsible for all contracting and contract management of the public IaaS providers, the contracts with the institution, receiving invoices from providers and invoicing the institutions.

3.4. SURFcumulus Basic

This is the version in which institutions will interact directly with one or more of the public cloud providers for the delivery of the IaaS services. SURFnet aids in the initial onboarding after which the institution uses the portal provided by the public IaaS provider for the provisioning and administration of the VMs. In case of incidents, the institution directly interacts with the public IaaS provider. This version is ideal for institutions who want to control everything themselves or who have a long-term contract for hardware or datacenters but want to use public IaaS providers for proof of concepts or bursting.

3.5. Cost recovery

As most NRENs, SURFnet is a not-for-profit and not-for-loss organization. SURFcumulus is positioned as a semi commodity service and should break even in three years. Meaning that all upfront investments must be recouped in later years.

There are two mechanisms which generate the income to cover the costs:

- A 5% surcharge on all usage covers all procurement, contracting (contract creation, data protection agreements, audit checks and operational contract management) and associated generic processes
- A subscription fee (starting at 40K euro annually) for the SURFcumulus Managed customers covers the SVP, CMP, 24/7 support and the SURFnet cloud Director group

Twice a year, SURFnet will check if the income generated by these two mechanisms reaches a point where the break-even is sustainably realized. If this is the case, these cost components will be lowered.

Adoption

SURFcumulus had a soft launch in July 2016 with the Cloud Management Portal, the SURFnet Virtualization platform and the Director team operational. The availability of the first set of public providers has created a lot of interest among Dutch institutions. Currently 7 institutions have signed up to SURFcumulus managed and this figure is likely to rise to 10 before the end of 2017. At the same time we see a lot of interest in the ‘do it yourself’ Basic version. The lack of upfront investments and not having to worry about procurements thresholds and security and privacy considerations has proven very appealing.

4. Annex 1: Rise and considerations

4.1. Origin

Six universities of applied science (Hogeschool van Arnhem and Nijmegen, Leiden, Hogeschool Inholland, Fontys, Saxion Hogeschool Utrecht and) had the desire to collaboratively run a joined ICT infrastructure services procurement. Recognizing that their needs are similar to those of other institutions, they approached SURFnet and created the Kube project (which led to the SURFcumulus service).

The goal was to organize to the procurement of ICT infrastructure services available to all institutions connected to SURFnet.

The desired service is described on the basis of four aspects (governance, legal, financial and service):

- The cooperation between the institutions and SURFnet is based on the relation between the affiliated members and SURF which means that SURFnet takes over the public tender responsibilities for the institutions and institutions can consume the services without running formal procurement projects or tenders.
- SURFnet acts as broker and Director of the service
- The services model is based primarily on IaaS (infrastructure as a Service) service as described in the SURF IaaS Proposition but is expected to (later) include PaaS and eventually SaaS services.
- The financial model is based on the principle of *pay per use* actually consumed ICT infrastructure services;

4.2. Reasoning

The following reasoning was used by the six Universities of Applied Science to seek a coordinated approach on Infrastructure services.

- Need for higher guaranteed availability as available through their own infrastructure
- Students and staff require IT services to be available 24/7. The higher education collective employment agreement don't allow for structural 24/7 support
- Many institutions don't regard having their own data centers as a core business for an educational institutions.
- Geographical resilience is highly desirable but is almost always deemed as excessively expensive
- IaaS services are complex in nature (contracting, privacy and security). Institutions don't have the skillsets to procure and manage these services.
- Infrastructure services require highly skilled engineers; institutions may be unable to find and employ these in the future.

4.3. Standardization

The basis for standardization and improvement of ICT services is the improvement and harmonization of the ICT infrastructure services. Think of higher availability of service and 7 x 24 hours support but also meeting higher requirements in terms of security, reliability, sustainability and flexibility. These requirements call for major investments if institutions were to realize those individually for their own institution. The members of SURF have to decide if they expect themselves to be able to achieve the medium-term delivery and continuous improvement of ICT infrastructure services. Is operating a datacenter a core business for an institution? It is expected that the necessary infrastructure services are already available on the market, but that it will take some years before suppliers can fully comply with the legal Standards higher education Cloud Services Framework on privacy and security.

4.4. Cloud development

The rise of cloud computing is the last years has gone so quickly that organizations struggle to keep up with its development, let alone that they will be able to match the functionalities with their own infrastructure at the same level of investment. The cloud providers offer various possibilities: ranging from services in a private environment, where it's clear where all data is and where the availability, security and thus the full internal management responsibilities are clear, to a public cloud solution in which this is the responsibility of the supplier.

In between on premise and full public provider usage there is the community cloud, where SURF-members can specify the required functionality and thereby also affect the security and privacy requirements. SURFcumulus Managed should be seen as a an example of such a community cloud service.

5. Annex 2: the GEANT IaaS procurement

GÉANT is Europe's collaboration on network and related e-infrastructure and services for the benefit of research and education, contributing to Europe's economic growth and competitiveness. The organisation develops, delivers and promotes advanced network and associated e-infrastructure services, and supports innovation and knowledge-sharing amongst its members, partners and the wider research and education networking community.

SURFnet is a member of GEANT and has taken a leading role in the intra-European IaaS procurement project in which a number of NRENs combined their resources to run a procurement which would allow over 10.000 research and education institutions in 36 countries to consume the cloud in a safe, easy and predictable way, with services that:

- meet European and national regulations
- have attractive pricing
- are connected to the community's networks and identity management capabilities
- can be purchased in a controlled and transparent manner.

By aggregating this demand from Europe's National Research and Education Networks (NRENs) and the 10,000 institutions they connect, GÉANT has created a substantial single digital market where up to €500m could be channeled through the framework contracts over the next four years. Furthermore, the portfolio of services and associated joint cloud delivery and adoption approach is delivering a firm basis for bringing the EC's European Cloud Initiative and European Open Science Cloud to fruition.

5.1. Getting all stakeholders aboard

In order to make a project like this a success, all stakeholders need to be on board and see the benefits. The procurement team invested heavily on this field by identifying the stakeholders and addressing their needs:

- Public Providers benefits are that they only have to answer to a single tender instead of thousands of them over the contract duration if institutions would tender individual. The team had meetings with all interested providers (collectively and individually) and shared the draft tender document at two stages asking them for feedback. As such, the public providers were aware of the why, how and what even before the tender was published.
- NRENs were informed of the projects and updated on the status at different conferences and meetings by the procurement team. The leading NRENs all contributed to the procurement team ensuring the internal awareness within those NRENs. All other European NRENs were explicitly asked if they wanted to participate in this tender; 36 signed up.
- The leading NRENs consulted their institutions, making them aware of what was coming and listening to their needs. The main benefits described to the institutions were:
    - Not having to tender themselves
    - Advantages of scale: better service guarantees and lower costs as when they would have tendered individually
    - Services which meet the strict legal requirements on privacy and security

5.2. Tender outcome

With strong interest in the tender, over 100 companies registered for the procurement. The following providers have qualified and will become available to European institutions.

- Amazon, through resellers: Arcus, Comparex, Telecom Italia,
- Cloudsigma
- Dimension Data
- Interoute
- itSoft
- KPN
- Lattelecom
- Microsoft, through resellers: Atea, Cacttus, Comparex, Dom-Daniel, Infosoft, Micromail, Nextsense, Novabase, SoftwareOne, Span and Ymens
- T-Systems
- Telecom Italia
- Vancis

Not all providers will be active in all countries. Some have opted to only respond to a specific set of countries while only a limited Microsoft and Amazon resellers are selected per country

5.3. Scope of Services

While the object of this framework agreement is primarily IaaS, other complementary service offerings utilizing Suppliers' Public IaaS resources may also be consumed. These complementary service offerings may not include co-location or SAAS services. All complementary services in Schedule 1 must utilize (or be based on or directly related to) the vendor's Public IaaS resources (CPU, memory, storage, networking).

Value added services e.g. Implementation services, Managed services or license based (e.g. VMs with applications pre-installed from a vendor's cloud "marketplace") services may be included but these must be a direct consequence of the usage of IAAS services. The value of services above IAAS services must not exceed 50% of the contract value over the duration of an award. This 50% limit does not include onboarding, architecture, design or related support services.

5.4. Complexity

Cloud services are extremely complex in (contracting and comparing) nature. It took an international team comprising of technical, procurement, business, marketing and legal experts two years to prepare and run the European procurement based tender and the resulting awarding and contracting. Individual institutions and even individual

NRENs will likely lack the expertise (and commitment) needed to do this themselves. Collaboration on an international scale is needed to realize this.

The GEANT IaaS procurement project has shown that, although European NRENs are in different stages of cloud adoption, the requirements for cloud services are generally the same among institutions in the different countries. As such, a future global effort in creating a collective set of requirements for specific types of cloud services will enable NRENs to collectively negotiate with public providers, making sure that the term and conditions meet the institution requirements.