NREN Cloud Strategy Guide

Supporting documentation for SA7, Task 1

Actual Date: 01-04-2015
Grant Agreement No.: 605243
Dissemination Level: PU (Public)

Authors: Slavko Gajin (AMRES/UoB), Robert Hackett (HEAnet), João Pagaime (FCCN), Diana Cresti (GARR), Fulvio Galeazzi (GARR) , Mary Grammatikou (GRNET/NTUA), Esmat Mirzamany (JISC), Simon Leinen (SWITCH)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Document Revision History

Version	Date	Description of change	Person
1	10-02-14	First draft	All
2	04-07-14	PESTLE analysis	Slavko Gajin
3	09-09-14	Text restructured, Strategy development process	Slavko Gajin
4	25-09-14	Scope of this Document, Additional details on risks, Funding model	Robert Hackett
5	20-10-14	Cloud provider model	Robert Hackett
6	14-11-14	Risks management	Slavko Gajin
7	15-12-14	Security section	Slavko Gajin
8	18-12-14	Executive summary	Fulvio Galeazzi
9	24-12-14	Deployment models, NREN roles, proof reading, Formatting	Slavko Gajin, Robert Hackett
10	16-01-15	Minor changes	All
11	19-01-15	Okeanos use case	Mary Grammatikou
12	23-02-15	Several other use cases	Diana Cresti
13	01-04-15	Summary section, merged contribution by Esmat	Fulvio Galeazzi
14	09-04-15	Proof-reading, final cosmetics, final version.	Fulvio Galeazzi

Table of Contents

1 Executive Summary

1.1 Motivation

In light of the emergence of Cloud Services in recent years and its recognition as an important topic for NRENs in a recent GÉANT survey, the GÉANT SA7 group has been tasked with assisting NRENs in adapting cloud services through a combination of task forces addressing key topics related to cloud such as strategy, brokering, integration and mobile.

The adoption and impact of cloud services on NREN clients cannot be ignored as it will change how they use NREN services and also their expectations. Vendors are investing heavily in cloud technology and services and it is forecasted that by 2020 a majority of NREN client's IT environment will be cloud based. In certain sectors this transition will be much more rapid depending on the benefits to clients and the barriers to adoption e.g. security concerns, legacy applications.

The recent GÉANT survey[1] carried out by the SA7 Cloud Strategy Task group has clearly identified that the majority of NRENs perceive cloud services as a fundamental shift which NRENs must recognise and adapt their business, service and even organisation models to accordingly. A key conclusion of the survey is that the "If or Why cloud" question is over and NRENs are now facing the questions of "what cloud services are required?" and "how to get there?".

The role of GÉANT SA7 is to actively help NRENs in the above activities with a highly collaborative approach to best support NRENs by:

- Helping NRENs form a bespoke strategy to meet their needs
- Sharing information on related technology, services, and business best practices topics and facilitating the replication/adoption of successful case studies through GÉANT community
- Brokering of agreements with service providers e.g. for special pricing or standardized contractual conditions
- Creation of a service catalogue of certified service providers
- Integration of public cloud services for peering or AAI i.e. eduGain

As a follow on to the survey, this document seeks to provide NRENs with a guide on how to address the issues and define a strategy and plan for their journey to the cloud.

NRENs have much in common, however there is no one solution for the approach to cloud services as NRENs differ in terms of political environment, funding model, resources & skillsets, appetite to risk, client requirements etc. As a result, this document seeks to highlight and provide insights into the key questions and issues rather than a prescriptive approach to the right or wrong way.

[1] https://intranet.GÉANT.net/SA7/T1/SA7%20Task%201%20documents/MS94_MS7%201%201_Cloud-Assessment-Document.pdf

1.2 Scope of this document

The objective of this document is to provide some guidelines to assist NREN organisations in their Strategy and Tactics in relation to Cloud Services. This document seeks to provide a toolkit based on the experience and lessons learned by NRENs and help identify or address key questions such as:

- What Cloud services should NRENs consider e.g. SaaS services such as VLE, CRM, IaaS such as Cloud Compute, Storage etc.
- Which deployment models e.g. Public, Private, Hybrid, Community
- Build vs Buy and the role of Brokering
- Operational model e.g. own resources, outsourced managed service
- Collaboration with other NRENs
- What will be the impact on the organisation e.g. resources and skillsets
- Business case and financial model, e.g., funding requirements

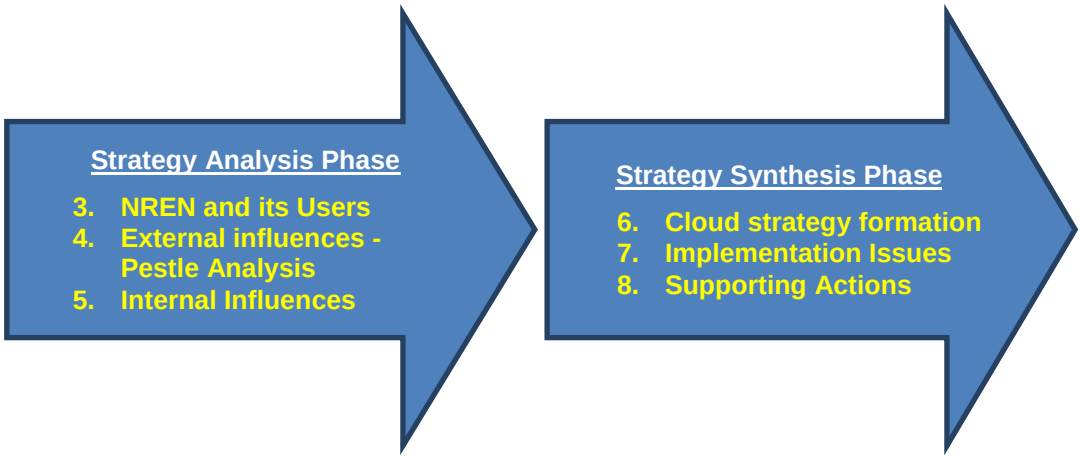
NRENs were created out of a community to serve the community's needs. Today those needs are evolving and it is being generally recognized that the NREN role should go up the stack, beyond "the wire". NREN's client organisations, i.e. research and educational institutions, are already faced with the cloud computing offering on the global market and many of them are already using public cloud services (such as email, collaboration and productivity tools).

Therefore, it is important for each NREN to define its attitude and strategic approach to cloud computing and take an active role in helping the user community in its uptake and use of cloud services for research and education.

The purpose of this document is to help guide NRENs in their journey to the cloud and how they can develop a Strategy for Cloud Services, covering two major phases:

- **Strategy Analysis Phase** i.e. the "What"
  - Analyse the NREN and its client's environment and requirements
  - Identify strategic goals
- **Strategy Synthesis Phase** – tactics to implement the strategy i.e. the "How"
  - Define & develop specific Cloud Services
  - Define business and service delivery models
  - Define organisational requirements
  - Develop a roadmap for implementation

The document is broadly structured along the guidelines above and Figure 1 provides a high-level roadmap to developing an NREN Cloud Strategy and maps the various phases and tasks onto the individual section numbers in this document.



The Analysis phase involves three levels:

- Understanding the users' perspective: their values, their needs, their business processes. This will provide insight into each user's possible advantages and benefits from adopting the cloud computing paradigm, as well as into the barriers and challenges which need to be faced.
- Understanding external influences, namely factors (drivers and constraints) external to the NREN which will affect the NREN in the context of cloud solution adoption The external influences can be broadly categorised into Political (alignment with European and national policies), Economic (costs and revenues, budget mechanisms, market competition), Social (user preferences, attitudes and perceptions), Technological (technology maturity, standards, service quality), Legal (data protection, compliance assurance) and Environmental.
- Understanding internal influences, the factors (trust, non-profit ethos, user-protection attitude, staff capabilities) constituting the unique internal strengths of the NREN supporting its capability to implement the strategy

The Strategy Synthesis phase needs to be based on the inputs from previously performed analysis and driven by user demands and business cases rather than technical challenges. The specific results of this process are the following choices and decisions that should shape the solution:

- Which user community is targeted - ordinary researchers, "long tail of sciences" researchers, teachers, students etc.?
- Which user needs are of interest to cover - commodity computing or high performance computing, storage or backup services, collaboration and productivity tools, eLearning, file sharing etc.?
- Which cloud service model(s) should be chosen – SaaS, PaaS, IaaS or some other?
- Which cloud deployment model to implement (public cloud, private/community cloud, hybrid cloud)
- What will be the role for commercial cloud providers?
- What is the appropriate role for the NREN?

As for the NREN role, several possibilities exist, such as: consultant, broker, owner or manager of externally-provided resources, and network peer. However, NREN clients' IT requirements are likely to require a variety of cloud solutions to deliver services in the future, and it is doubtful that all the answers to such requirements may

be provided by a single solution or vendor. The future landscape is likely to consist of a "multi-cloud" environment, which will require the NRENs to adopt a multi-layered approach.

The Strategy Synthesis phase should also define the roadmap to implement the strategy, which would consist of the following three phases:

- Preparation phase – including activities to prepare the project team, establish budget and procurement, as well as technical activities to specify technical requirements, acceptance criteria, and design the service with all necessary details to achieve the specification.
- Implementation phase – including activities needed to bring the service live (conducting the procurement, technical installation, configuration, testing and onboarding) as well as supporting activities, such as project management.
- Operation phase – including long term activities such as day to day service operation, monitoring, reporting, maintenance, support, helpdesk, training, promotion marketing etc.

The implementation of the strategy should include, since its earliest phase, a thorough consideration of the security aspects involved. This can proceed along a categorization of the security issues (for example, the one proposed by the Cloud Security Alliance), and it is important that for each class of security issues both the perspective of the users of cloud services, as well as the perspective of the cloud provider (also when the NREN acts as a cloud broker) be discussed, and the demarcation border between the respective responsibilities (users, NREN and commercial provider, if applicable) be clearly identified.

Implementation of a cloud strategy is likely to be challenging due to the potential risks involved regardless to how the plan is well defined and detailed. Risk management is therefore an essential part of the project plan which deals with the undesirable events that might occur and affect the project results, time plan and money. Cloud strategy therefore needs to include proper risk management in order to anticipate possible risks in an early phase, analyse their impact, and plan mitigation approaches. The goal is to minimize the negative impacts of these unwanted events if they occur, take better decisions and, if possible, turn them into opportunities. To do so, the risk management approach needs to identify possible risks and develop corresponding actions that are incorporated into the initial project plan and budget.

Last, but not least, the Strategy Synthesis phase should also address a number of supporting actions which are crucial to successful implementation of the strategy, like:

- Organizational changes: developing and evolving internal competencies (in as diverse fields as technical, commercial, legal, contractual)
- Cloud financial model: although the NREN cannot and should not directly compete with the public cloud providers, there may be an opportunity for the NREN to provide a differentiated service to its users for example by offering a simpler, more transparent financial model. Such a model involves the following key elements:
    - funding availability and constraints to providing cloud services,
    - pricing model, taking into account individual costs of all users' requirements (IP addresses, network traffic, database I/O, DNS queries) as well as "hidden" costs (data security and privacy, federation, network)
    - billing model, which may be required to match additional requirements in terms of reporting, volume or time-span discounts, possibility to integrate with external billing or reporting systems.
- Service branding and key messages, leveraging information about users gathered during the Strategy Analysis phase
- Service Assurance. The demands of the many and varied use-cases are likely to vary from low end, commodity and best effort requirements, to high end computing, mass storage and business critical

requirement: cloud services, while new and perhaps different to more traditional services, should in many cases be able to fit in with an established service environment with limited impact.

The definition of the NREN Strategy toward clouds should be regarded as a highly dynamic process. In this document we have tried to provide the elements to help each NREN draw a recursive path running through the following steps: Observation, Planning, Doing, Checking, Adjusting.

Once the cloud strategy has been setup it is very important to communicate it (not necessarily through a formal document) both internally within the NREN and externally to (potential) users, so as to share the key messages with the main stakeholders: “why” is the NREN getting involved with clouds, “who” is the community addressed by the offer, “what” are the available services, “how” the services will be provided (technical and legal aspects, SLA, resulting benefits,…).

Finally, in the last part of this document we have collected a set of recommendations and a varied set of “Inspiring Stories”, representing the essence of the experiences of some NRENs in the field of clouds. Although the landscapes in which NRENs operate differ tremendously, we are confident that this last element nicely complements the rest of the document, which we hope you will find useful to make your journey to the cloud successful and safe, for your organization and your users.

2 Background

The role of the NREN is not static and is influenced by the economic and political realities, as well as new opportunities (and threats) afforded by new technologies. NRENs were created out of a community to serve the community's needs. Today those needs are evolving and it is being generally recognized that the NREN role should go up the stack, beyond "the wire". On the other hand, the "selling point" of the NREN is less and less related to its uniqueness as network provider, but should be connected with other specific features not (at all, or not economically) available via commercial providers.

The explosion of the cloud phenomenon over recent years, which has brought users the possibility to acquire and consume high-quality services in an innovative way, is at the same time bringing the need to handle an increasing data volume which is produced and exchanged ubiquitously using a number of devices. For this reason the NRENs, who have always been at the forefront of technological excellence, can hardly regard the cloud as mere spectators.

By its nature, the scale of the cloud phenomenon is trans-national, European at least. At the same time, over last ten years there has been, in the field of scientific and technological research, a proliferation of large scale initiatives also in sectors where this was not traditionally the case (ESFRI projects).

On the other hand, NREN's users, i.e. research and educational institutions, are faced with the cloud computing offering on the global market. Many of them are already using public cloud services (such as email, collaboration and productivity tools), some have implemented local cloud provisioning (mostly IaaS based on virtualized computing resources allocated on demand), some are planning to deal with cloud services in the near future, while others are still unaware, uninterested or puzzled about the potential of cloud computing.

Therefore, it is important for each NREN to define its attitude to cloud computing and take an active role in helping the user community to adopt and use cloud services for research and education. It could be done by providing cloud services for the community, brokering cloud services by aggregating user demands and negotiating with cloud providers on the global market, or at least supporting the users to adapt cloud services by itself. This is a process which requires thorough analysis, planning and decision making, most probably resulting in changes in the organization (skills, technology, business model, working practice etc.) and possibly significant investment in time and money with long term consequences.

For the above reasons, it is important for each NREN to define its approach to dealing with cloud computing and position its role in providing users with cloud services for research and education in the form of a medium-term strategy.

Generally speaking, defining a strategy is an analytical process, which consists of two major phases – a *Strategy Analysis Phase* and *Strategy Synthesis Phase*, with the following purpose:

- to specify the strategic goals to be accomplished,
- to develop a roadmap and action plans to achieve these goals, and
- to define resources to be allocated to implement the plans.

To start with the analysis phase, the NREN must gather information from various sources and different stakeholders to be analysed in order to define strategic goals. This analytical process involves the following:

- Understanding the values of key stakeholders (research and educational organizations, individual users, ministries, funding bodies, NREN itself);

- Understanding user business processes, which are primarily addressing research and education activities;
- Analyse user needs and demands in relation to the potential of cloud service;
- Analyse drivers and benefits of using various cloud services from the user perspective;
- Analyse potential issues which need to be resolved in order to exploit the benefits;
- Analyse potential risks that could be associated with the use of cloud services.

In addition to the above analysis, which mostly addresses the user perspective, further analysis need to be conducted from the NREN perspective, acting in its role as a national e-infrastructure provider for the research and education community. This additional analysis includes:

- External influences, which affect drivers and constraints to implementing the strategy, consisting of many aspects, such as political, economic, social, technological, legal and environmental;
- Internal influences, addressing NREN capabilities to implement the strategy, including internal strength and weaknesses.

And finally, potential cloud solutions and existing offerings need to be analysed to complete the picture and capture all possibilities and options. In the case of an NREN provisioning its own cloud services (private/community/hybrid cloud), the technological aspect is the main concern at this analysis stage, which needs to address how it matches the previously analysed user requirements and other issues. The analysis of public cloud solutions which are available on the market is also necessary, especially in the case where the NREN is considering a brokering role in order to help the wide user community to adopt public cloud services.

Once the thorough analysis is completed, producing insights and an understanding of “the whole picture”, many questions will still need to be answered, dilemmas resolved and decisions made, and this is the focus of the next stage - the strategy synthesis phase. This phase is more about strategy synthesis, by developing business cases in the form of goals and implementation scenarios to achieve these goals, which needs to validate if the implementation is realistic, achievable and cost effective. The Strategy Synthesis phase is an iterative process of strategic thinking with feedback loops intended to create the most preferred solution which provides the best opportunities and maximum advantages. This process needs to identify:

- Which parts of the user community are targeted: ordinary researchers, “long tail of sciences” researchers, teachers, students etc.?
- Which user needs will be matched: commodity computing or high performance computing, storage or backup services, collaboration and productivity tools, eLearning, file sharing etc.?
- What cloud service model(s) should be offered to what part of the user community – SaaS, PaaS, IaaS.
- Which cloud deployment model will be established – Private cloud, Community cloud, Hybrid cloud, Public cloud
- What will be the NREN role in the cloud service provisioning – cloud provider, cloud broker or manager of external resources, consultant or network peer.

Based on the defined goals, implementation scenarios and decisions taken in relation to the aforementioned questions, a cloud strategy development should be further extended into the definition of a roadmap and detailed action plans to achieve these goals. This strategic planning process needs to consider all the resources which are required to be mobilized to implement the strategy, such as:

- Personnel spanning a broad range of expertise: system administrators, network engineers, security specialists, software developers, legal experts, procurement staff etc.
- Timescales to implement the strategy, which need to be estimated, planned and well organized
- Funding required to establish the cloud services, especially in the case of implementing an NREN cloud service for its user community.

Even with the most comprehensive strategy and planning, there is a real risk for every plan that things may go wrong during the implementation phase. A detailed risk assessment therefore needs to be carried out in order to identify, analyse and evaluate risks and manage them by taking actions aimed at avoiding, transferring or at least keeping them to an acceptable level.

3 NREN and its Users

The NREN's core activities are in providing network and associated services to its user community that usually comprises:

- Higher education institutions and possibly other levels of education;
- Research institutions, for instance, universities or state laboratories;
- State agencies or financing bodies.

The above characterization is general and is not intended to be exhaustive, but is nevertheless useful to establish a context for the rest of the chapter.

3.1 User needs and demands

The user community in a typical organisation will generate a demand for general computing resources to meet common requirements such as email, office productivity applications, video-conferencing, storage, file print and share, CRM, database hosting, web-hosting and the typical needs common to most organisations.

In the educational and research community there is also a significant need for more specialized computing and storage resources, for science computing or engineering, that is driven by use-cases specific to the nature of work carried out by the sector. There are a number of typical user scenarios which have very specific and often very demanding requirements e.g. running scientific experiments that are CPU or network bound applications. GRID computing projects and, more recently, cloud computing projects, emerging from the educational and research community.

The following differences are found between the requirements of the two user communities:

General computing:	Science computing:
• Requirements are common to many organizations • Load varies on daily and weekly cycles e.g. low night use. • Availability may be critical for business normal functions • Long term predictable usecases (stable configuration and requirements)	• Requirements, like performance, are specific • Load is high during scientific experiments that can take weeks • Availability isn't usually critical (experiments can be restarted a day in the near future) • Configurations may vary dramatically according to running experiments

These two user environments within the typical NREN client base have very different requirements and possibly different solutions, so in defining the NREN strategy for cloud services, it is recommended to carefully consider these different requirements.

3.2 Advantages and benefits

The list of potential advantages and benefits of using cloud computing is outlined below.

It is a list of the generally accepted reasons for adopting cloud computing services, but needs to be analysed from the NREN client organisation perspective in relation to the specific business processes and the organizational context in which they operate. Aside from general computing capabilities, which are always needed, the research and educational activities bring additional requirements but also opportunities and challenges to exploit the potential benefits of cloud computing. The analysis performed by an individual NREN may well lead to an extension of this list with additional advantages and benefits that are specific to particular user communities in some countries.

- **Cost effective** – The most obvious advantage of cloud computing is significant reduction of capital investment. From the perspective of research projects the financing is well balanced, moving the funding from capital investment to operational cost (from CAPEX to OPEX) and exploiting “pay-as-you-go” and “on-demand” payment model. With this approach the projects are more competitive in terms of cost with less financial risks. Nonetheless, the organization still needs to initially invest in preparing for the cloud, which involves the cost (in time and money) of configuring and implementing cloud services, integration with internal in-house systems as well as internal organizational changes.
- **Easy and fast deployment (more agility)** - Implementation of cloud services is much faster and easier than traditional IT, helping organisations become more agile and responsive to the needs of the business. It is no longer necessary to wait weeks or months to purchase, install and configure computing equipment, to bring the system/application/service alive. The researchers can focus more efficiently on pure research and scientific activities and innovation. Reduced time for resource provisioning and setting up of the environment allows early testing of scientific ideas with faster “time-to-value” effect and reducing the time required to manage infrastructure requirements e.g. servers. The advantage is obvious in the educational area as well. For example, students can also easily and quickly obtain the resources to complete their educational activities (for instance lab exercise) and release it after that.
- **More flexibility and scalability** – Research projects and scientific experiments often require capacity which is not always predictable: in a cloud based environment this is not a concern as users can easily increase and decrease capacity (processing power, storage, number of virtual machines). The flexibility of cloud services allows dynamic and rapid on-demand or even automatic scale up of the capacity during the period when it is required. In the same way, the capacity can be quickly released when it is no longer required. The ability to provide resources in any quantity at any time often results in a user perception that the cloud capacity is almost unlimited. However, most scientific algorithms do not scale linearly and adding more resources cannot always solve more complex problem. Moving to a cloud environment, therefore, can require the optimisation of existing application programming to exploit the full benefits of cloud computing.
- **Ease of use and access** – Although it depends on the service model chosen, one of the basic benefits and business drivers of cloud computing is simplified usage and universal access from any location with Internet connectivity. These characteristics result in improved productivity in the science and research areas, and more efficient learning environments for educational organizations (universities, schools). The adoption of Cloud services can be expected to change the working practices of users, mostly in positive ways, but can also introduce new demands such as support for mobile devices, improved identity management or VPN access.

- **Improved business processes** – the benefits discussed previously also facilitate improved business processes in user organizations. Instead of spending time and money on in-house deployment of business applications, many of those applications are now available as cloud services. With improved accessibility and data sharing in real time from any location, collaboration is improved both internally in the organization and externally with other local or international partners, such as a pan-European project consortium (for instance in the context of Horizon 2020).
- **Energy efficient** – one of the benefits of using outsourced IT capacity in a user organisation is the financial benefit of reduced energy utilisation, but a cloud service provider can also optimise the power consumption. Virtualization can dramatically increase the overall computing utilisation, while cloud services go even further. The adoption of cloud computing results in more optimised usage of computing resources which leads to reduced power consumption. The benefit is even greater bearing in mind that the single biggest driver of power consumption in a data centre is the need for cooling. Owing to the centralization of computing resources and, as a consequence, the fact that the energy consumption is moved away from (smallish) user organizations, a cloud service provider is in a better position to build and organize its data centres in more efficient ways, potentially using renewable energy. Cloud computing thus contributes to the greening of the global ICT world.
- **Business continuity** – The continuity of business processes in the case of failure is an imperative for many applications. Instead of investing in a disaster recovery facility, significant cost saving can be achieved using external cloud services, which inherently provide high availability and reliability. A barrier to this is that core critical applications, which mostly require strong business continuity, are not always suitable to be moved into a cloud environment, especially public cloud. Therefore, there is room for an NREN as a competent partner for the research and education community, to help user organizations by providing solutions. Currently, the data protection policies and compliance provided with cloud services needs to be improved significantly to meet the requirements of the research and education community.
- **Internal IT transformation** – The use of cloud services by user organizations releases the need for some IT jobs, mostly in system administrations. The organization can lower the operational cost for IT maintenance or rather shift IT focus from system/service administration and maintenance to more valuable tasks such as innovation and support to core business process.

3.3 Barriers and challenges

This section highlights some of the barriers, challenges and risks exposed to NRENs and its clients when adopting a cloud computing service. These factors need to be identified and considered in the NREN cloud strategy and if possible resolved in the implementation phase in order to exploit the benefits of cloud services.

- **Security** - Cloud services and technologies have continued to evolve rapidly but have also brought new security challenges, which is the biggest single concern of most organisations in the adoption of cloud services. When data and processes are outsourced to the cloud a significant part of the control and responsibility is removed from the organization and transferred to the cloud provider. EU and National Regulators, as well as vendors and standards bodies such as the Cloud Security Alliance (CSA) are working to address the requirements, however new standards and security best practices have not kept pace. The CSA has identified 14 domains to be addressed as part of its security guidance in Cloud Computing, but from the users' point of view the areas of biggest concern are the following:

- Legal and compliance challenges, such as security breach disclosure laws, regulatory requirements, privacy requirements, international laws, intellectual property etc.
- Information management, including data confidentiality, integrity, and availability, data protection, especially protection of personal data
- Identity and access management – since the cloud services are accessible from anywhere and usually are organized in a multitenant environment, users are concerned about how identity and access protection is provided and managed by cloud providers
- Business continuity is a concern when moving critical processes to the cloud, and includes concerns about cloud provider system resilience to deal with a disruption, disaster recovery and restoration processes etc.

- **Compliance with existing policies** – Using cloud services often involves the outsourcing of sensitive information to the provider's physical location. The concern is significantly higher if the cloud infrastructure is located in a different country under different legal jurisdiction. The sensitive information in this case can be personal data, financial data, students' records, research data and so on. This new cloud oriented approach can be inconsistent with the existing standards such as ISO9000 or ISO27000, or an existing security policy not originally designed to apply to cloud environments. In this case, some data protection and information security processes are moved to the cloud provider who must fulfil the requirements for compliance to the standards.
- **Resistance to new working practices** – Technological changes, such as the adoption of cloud computing, may affect existing work practices. Most of the consequences have a positive impact however some resistance to new ways of working may occur, as it may require new roles, responsibilities and skills. User institutions need to consider and address potential resistance and undertake measures (policies and procedures) to support staff to overcome negative perceptions, upgrade the relevant skills and build the confidence to adapt to new working environments in an effective way.
- **Lack of control** – Moving information and processes to the cloud may involve a significant part of existing responsibilities and control being transferred to the cloud provider. In general, the higher the cloud service in question is in the deployment stack (going up from IaaS to SaaS) the less control remains with the user over the information management. The reduction in control, relates not only to user perception, but also to the practical need to monitor system performance and data integrity, the ability to access the system management plane to log user activities and system events in order to troubleshoot problems and audit security etc.
- **Internal IT transformation** – The above mentioned benefit of internal transformation of the IT department could be a barrier or at least a challenge for both organization management and IT staff. Using cloud services instead of traditional IT systems may lead to possible IT staff reduction, which will raise staff concerns in relation to job security and result in internal resistance to change. Aside from lowering the cost of IT operation by adopting cloud services, losing in-house IT skills, experience and capacity built up over time, in the long run could lead the organization into a position that would be very difficult and expensive to revert back.
- **Integration with in-house systems** – Cloud Services in general need to co-exist and integrate with other NREN business and IT systems e.g. networks, management & monitoring, backup systems, security systems, federation etc. Cloud services also need to meet compliance to in-house IT and service level delivery requirements if they are to be used in a production capacity. The testing and integration work to bring cloud services into the catalogue of NREN IT services may require significant time and effort and will vary from NREN to NREN.

- **Technology immaturity** - Cloud technologies are evolving rapidly but are generally regarded as immature except in the case of some of the major SaaS providers. Many products or services for example are relatively new and unproven. There have been many high profile failures with some of the largest public cloud service providers despite their resources and capabilities. Similarly, standards, e.g. for security or interoperability, are lagging behind the reality of technology and services and are still in development.
- **Vendor lock-in** - As a new technological model and emerging services market, cloud computing is still faced with the lack of standardization and readiness of commercial cloud providers to fully support interoperability. On the other hand, it is very realistic that a user sooner or later will need to switch to another cloud provider, for a number of possible reasons such as lack of satisfactory service quality, increases in cost, business disruption or inability of the cloud provider to follow the technology improvements and market competition. Without standards for interoperability between different providers and vendors, the users are exposed to the risk of being locked-in to a specific cloud provider with limited or no choices or freedom to move to another one and to meet new business requirements. Even with the interoperability standards in place, changing a cloud provider is not an easy process, which assumes migration of user data, application and business processes. The objective is to try in so far as is possible to ensure the potential for interoperability and vendor independent migration of service with minimal amount of manual work and time to transit to new provider.
- **Resources and skillsets** - Depending on the NREN strategy e.g. to build or buy cloud services, the requirement for resources and specialised skillsets may vary but include some or all of the following:
    - Legal and contractual expertise
    - Service Management
    - Technical expertise (cloud operating systems and tools)
    - Security Management
    - Billing and commercial
- **Funding risk** - Cloud services in general require complex infrastructure, significant resources and skillsets and consequently significant funding. The startup costs to build a new service may be high and the funding for this may pose a major barrier to progress. In this case, brokering of services, with other NRENs or cloud service providers, may be attractive. For cloud service providers different models are being offered e.g.
    - Use the public cloud, e.g. through specific agreements brokered by GÉANT
    - Use a public provider to provide a virtual cloud within its datacentre reserved for NREN clients and operated by the cloud provider as a managed service
    - Use a service provider to build and operate a cloud service hosted in the NREN infrastructure.
- **Commercial risk** - Cloud services are dynamic in nature with the consequent impact on revenue, which makes the NREN business case difficult to predict. The pace of adoption by NREN clients may be unpredictable depending on their use cases and other factors. To mitigate against this, one approach is for NRENs to reduce risk by taking a Pilot or Proof of Concept approach to allow clients to test use cases, gain experience and provide feedback to demand (and hence service income) to a future production service.

4 External influences – PESTLE Analysis

A PESTLE analysis is a useful tool to support the investigation and decision process relating to cloud services. PESTLE in general covers Political, Economic, Social, Technological, Legal and Environmental issues in the strategic planning process. Its outcomes identify drivers and constraints through external influences which affect the NREN in context of cloud solution adopting. Each of these aspects of the cloud business cases are covered in the following sections.

4.1 Political influences

The NREN cloud strategy should be aligned with the European and national policies, but also with the strategies of the member institutions.

4.1.1 European Policy

The European Commission have already recognised the potential of adopting cloud computing among a wide range of sectors. The Communication from the Commission to the European Parliament [14] puts forward that the digital single market, the first of seven pillars of a Digital Agenda, can be raised to a new level by using cloud computing services. Specific key actions have been set up to stimulate active adoption of cloud computing towards making Europe cloud-active and cloud-friendly. This is especially relevant to the sectors of science, research and education. The European Commission Digital Agenda which is part of the overall Research and Innovation Action Area, underlines the need for a European wide strategy on cloud computing, that considers economic, legal and institutional aspects. While the many benefits of cloud services can further drive science, innovation and education, various barriers still exist and must be resolved in order to realise the benefits. Priority actions for policymakers have been identified to take measures to remove existing barriers and further facilitate the acceptance and usage of cloud services.

The e-Infrastructure Reflection Group (e-IRG) in its study “Cloud Computing for research and science” [5] makes the recommendation to integrate several e-Infrastructures components, including cloud initiatives to facilitate a single point of access to European Research Area.

Horizon 2020 programme will also promote and facilitate not only adoption and uptake of cloud computing, but also research and development of various cloud services and business models for its usage.

4.1.2 National Policies

While the European Commission policy presents a common framework that all NRENs can rely on, there is diversity across the national environment in which NRENs are operating. In more developed countries the trend is to integrate network infrastructure, computing infrastructure and data infrastructure into a single entity, named e-Infrastructure, to facilitate research, science and education. To this end, cloud computing is a new paradigm which brings new technologies, services and business models into computing infrastructure solutions

which supplement the established solutions such as grid computing, high performance computing (HPC), and high throughput computing (HTC).

Some countries already have a national strategy addressing Research Infrastructure and a roadmap for the adoption of cloud computing as a part of e-Infrastructures for science, research and education. In other countries this process is still on-going or in the early phase of the establishment. The recommendation from various EU policy documents and studies is to support the uptake of cloud computing and its integration into e-Infrastructure to maximise the benefits in various sectors, such as government, science and education. However, the necessary policies, rules and legal framework for cloud computing are not yet fully defined.

NRENs are widely recognized as the main pillars of national e-Infrastructures. The recent cloud computing questionnaire, carried out by the GÉANT SA7 Cloud Strategy [13], shows the relevance of cloud services for the NRENs, where two-thirds of the respondents indicate that cloud services impact their organization. From the e-Infranet project[2], some countries already have a roadmap to deploy a national cloud infrastructure for research, while several others have on-going pilot projects in cloud computing initiated by NRENs, universities, and other research institutes. Noteworthy, in these cases the participants were ready to collaborate in the establishment of cloud for research at the European level.

Taking into account at a macro level the many initiatives and drivers towards cloud services, it would be unwise for NRENs to avoid dealing with cloud computing: NRENs would rather need to carefully consider their position and approach. To take a more proactive approach, NRENs should align their strategy, planning and development activities for cloud in line with the national strategy. In those countries where a specific strategy does not exist, it may be an opportunity for the NREN to play a leading role to drive and shape the national policy and strategy in the state-of-the-art technology. The examples are network development in last decades or recent GRID/HPC/HTC initiatives. Therefore developing a cloud strategy in collaboration with the national policymakers in this area could be very beneficial for the wider community.

4.1.3 Institutional strategies

Universities, research institutes and other third level institutes form the core user group within each NREN. Most of them have a strong demand for research computing facilities. The institutes traditionally invest in their own equipment and additional overhead to support its operation. The growth of cloud services on a global basis have created new alternatives for each institute to the traditional approach which in many cases will lead to change in its internal policies and attitude towards outsourced computing resources and services in the cloud. Recent studies show that the institutions are increasingly considering the potential of cloud solutions as a part of their internal strategy and ICT development. Non-core business processes, application and information, such as email, document management, collaboration tools, backup storage etc., in many cases have already been identified to be moved to the cloud service providers since they can provide more flexible, cheaper, effective and in many cases better functionality. For non-commodity services however, such as the core business processes, corporate applications and data, information systems, financial data, student registry etc., a far greater degree of caution is being applied by institutions in relation to the potential risks and business impact that might arise from moving to a third party cloud environment. An additional barrier to using cloud computing in research institutions is the fact that many of the existing business, educational and research applications need to be adapted before they can be migrated to cloud environments.

[2] http://e-infranet.eu/

The institutional attitude and new initiatives towards cloud services can be an additional driving force for the NREN to work on its cloud computing strategy in order to offer them new business models and solutions.

4.2 Economic influences

4.2.1 Budgetary constraints

The recent financial crises will be influencing national economies for the foreseeable future in many countries. Budgetary allocation for science and research in more developed economies is up to 3% of GDP while in less developed countries it is often ten times less (0.3% of GDP and lower). Bearing in mind the variation of GDP among European countries, the consequent variation of the actual total investments in research and education sector is even greater. However, everybody shares the position that innovative research and education are major economic drivers on long term.

On the other hand the information technology and associated resources, which are a mandatory part in this process, are not cheap. Faced with a reduced budget it is not easy to invest in research and education computing facilities and potentially wait for years until the results become visible. This makes the research and education sector more fragile during the economic downturn with the consequent budgetary constraints.

However, the reality of budgetary constraints and reduced investment in the research and education sector can also be drivers towards the adoption of cloud services if the technology can bring a new cost saving model. In light of this, cloud computing may provide some new and promising options for institutions in meeting the needs of their business. This alternative approach needs to be considered and balanced with traditional institution-based computing services. Instead of investing in their own computing infrastructure, institutions may be able to achieve significant cost savings by using computing resources on demand, whether these resources are shared by other institutions at the national level or purchased on the global cloud market.

4.2.2 Hidden costs

While the capital expenditure can be avoided using cloud computing, there are still other hidden costs involved in preparing and implementing IT services for the cloud and integration of cloud services with existing business processes. The cloud services have the potential to scale computing and storage capacity easily and elastically on demand. However, most scientific computing tasks do not scale linearly. Adding more resources to the task in this case will increase the cost without necessarily achieving the expected result. Existing programming code and applications may often need to be changed and improved to work effectively in a cloud environment, which is a time consuming task for the researchers and IT staff resulting in increased indirect costs.

4.2.3 Budgetary mechanism and funding sources

Budgetary mechanisms and funding sources can also affect the uptake of cloud computing within research and education community. Funding bodies are generally not very familiar with technology, as in this case with the benefits of using cloud computing, and can be expected to resist changes to the existing funding model. On the

other hand, researchers have a tendency to control their own grant budget for purchasing IT resources (equipment and services) independently of institutional policy. The success of moving IT services to cloud solutions at a national level depends not only on the NREN itself, but also on the commitment and involvement of all stakeholders, including funding bodies, institutions and individuals. Therefore NRENs should propose the best value for money business model and promote it among all parties.

4.2.4 Payment model

According to the TERENA compendium[3] there is a wide range of models in how the member institutions are funded for NREN operation and the services they provide. Some NRENs charge 100% of the cost to member institutions while other NRENs offer all the services for free, fully covering operational NREN costs only from the State budget. Between these two extremes there is almost linear scale of participation fees in percentage from 0% to 100% for the amount that member institutions contribute to total NREN budget.

Adding new services based on cloud solutions is expected to be consistent with the existing NREN funding models. The specific cloud deployment model (NREN private cloud, broker for third-party cloud, peering to major public cloud providers) will also affect how the funding model will be established. In any case the flexibility of cloud services can fit to any payment model whether it is fully free, fixed price, or based on a pay-as-you-go model.

4.2.5 Cloud market and Services

Cloud services are already extensively used by the research and education community and a wide range of NREN users. Many institutions have already moved some services to the commercial cloud environment e.g. Gmail, Microsoft Office365. The most common examples are the adoption of email services for users, or provisioning computer and storage resources with cloud providers.

This situation strongly affects the NREN position in establishing new cloud services and the business model for NREN members. NREN cannot and should not compete directly with the public cloud providers. Instead, NRENs should identify technological benefits, value added services and a business model which can best serve the institutions' needs and interests. Integration with the existing NREN services, such as AAI federation, could be an example of a key differentiator. Another NREN advantage is existing collaboration with the community, based on previously established trust.

In the event that an institution decides to move the services from the public cloud environment back to an NREN or to any other cloud solution, this is likely to be a very difficult and expensive process. The most serious problem is lack of interoperability which can lead the institution to a vendor lock-in trap. This is a very realistic problem which should be a major concern for NRENs and their clients and additional motivation to the development of a cloud strategy to support the user community needs and demands.

[3] www.terena.org/activities/compendium

4.3 Social influences

4.3.1 User preferences

The broader user community has already accepted cloud services, which is especially true for free and commonly used public services, such as web-mail, productivity tools, file sync and sharing services, communication tools and so on. The fact that the NREN users already have their own preferences, will strongly influence NREN decisions with regard to which cloud solutions should be considered for deployment.

This situation demonstrates that users are already very familiar with the cloud environment and would likely accept new cloud-based services if they are offered or brokered by NRENs. It is difficult, if not impossible, to compete with commercial cloud providers and free services due to their scale and so NRENs are challenged to find a new value-added model and services for both individuals and member organizations.

4.3.2 Local culture and attitudes

The local culture in the usage of ICT services and the user attitudes in different countries or different sectors can also affect the uptake of cloud computing. There is a common perception and widely accepted attitude that the flexibility of ICT services involves a risk if it is not tangibly and physically controlled by the organization. These doubts and negative perception of cloud computing services can be partly justified if other aspects of cloud environment are not carefully addressed. The most important aspects to consider are technological issues and the legal requirements (see the subsection 4.5).

4.3.3 Ownership

The perception about ownership of computing resources at institution level will affect the NREN strategy in cloud service provisioning. Ownership and control of powerful computer facilities gives the institution prestige compared to other institutions in the community, demonstrating institutional commitment to ICT. It is an important factor in competition within the sector which could lead to attracting the best researchers, providing more funding and getting more research projects.

NRENs should consider this factor, which is not only in contrast to the concept of cloud computing, but often in contrast to optimal cost-effective solutions, while promoting adoption of cloud services among their members.

4.3.4 Accessibility

One of the greatest benefits of cloud services is the ability to access the services from anywhere and anytime. Researchers can access their data and continue the research at home, teachers can upload the learning material, and students can access it from anywhere without dealing with firewall or VPN network access. It brings a substantial flexibility for the users, but also exposes the service and data to potential security risks.

In addition to the “anywhere, anytime” nature of the accessibility, today’s user perceptions and expectations are also increasing and assume access “from any device”. In providing a cloud service, NRENs can expect such demands, which could bring additional technological challenges and increase the complexity.

4.4 Technological influences

The benefits of cloud technology are evident and well known: flexibility, scalability, reliability, portability, on demand usage, pay as you go, ease of use etc. In contrast to these benefits which strongly drive the uptake of cloud computing, the sections below highlight other issues which create barriers and limitations in the uptake of cloud computing.

4.4.1 Maturity of the technology

Cloud computing is an emerging technology model which is already here and it will continue to change, both in terms of technology and business model. The institutions’ concern about maturity of cloud technology will also influence their decision whether to exploit the benefits of cloud services or keep with the traditional equipment-based approach.

Lightweight and ease of use cloud services will be more easily accepted by the community. On the other hand, if the implementation of cloud solutions requires deep technical knowledge that the institutions need to provide, it is less likely that the service will be accepted easily and adopted successfully.

NRENs can play an important role in testing the maturity of cloud technology by implementing pilot services and work with the community to find the best deployment model.

4.4.2 Standardisation and interoperability

Lack of standardization is identified as one of the major concerns with regard to the cloud computing business model and usage. Without widely accepted standards and the support of the biggest cloud providers, the ability to move data and services between vendors will be very limited and practically impossible. Therefore interoperability is an open issue which still needs to be solved to avoid the risks of vendor lock-in. The European Commission strongly supports the standardization process based on open source platforms, but the question is still how the global market, directed by the biggest providers, will address this important issue in the future.

4.4.3 Service reliability and quality

The more critical the data and processes for a particular service, the greater the degree of concern and caution there will be for an institution considering its migration to the cloud. Another important factor which raises concerns is the number of users, which is generally high for cloud services and making any service disruption highly visible. Obviously, the service reliability and quality need to be provided at the highest level as any downtime, even for maintenance purposes, would lead to negative user perception.

A Service Level Agreement (SLA) therefore defines a guaranteed level of reliability and quality that the users can rely on. Realistic but acceptable service levels needs to be defined, taking into account all external and internal factors and dependencies, such as the network, power supply, system support, AAI, etc. This is a challenging task for NRENs, but proper SLA monitoring and user reporting will help NRENs to achieve this level of the service.

4.4.4 Existing Infrastructure

Cloud services are typically established on the top of the existing infrastructure stack, and may include a system layer (such as a virtualized platform), middleware (such as AAI) and network infrastructure. Regardless of which cloud deployment model research and educational institutions are using (own private cloud, NREN private cloud, public cloud etc.), the GÉANT and NREN network infrastructure plays an important role. High network quality, both on access and backbone layers, is required, and this is the place where the NREN strengths naturally come into play. Providing high network bandwidth is always positive, especially for those cloud services which are very intensive in terms of data transfer, such as storage and file sync and share services. On the other hand, cloud services which are more interactive may only require low network latency.

4.5 Legal influences

4.5.1 Legislation

NRENs need to ensure they are aware of and compliant with national and EU level regulations. In most cases the legislation addresses not only data ownership but also its locality, which is in contrast to one of the fundamental principles of cloud (“could be anywhere”). Thus, it is likely to include for example measures to ensure data protection and data location is assured and that appropriate policies are defined and enforced as well as the appropriate security mechanisms, standards compliance such as ISO27001/2 including independent auditing being in place.

While NRENs and its member research and educational institutions operate under European and local legislation, most public cloud providers operate globally. The problem appears when the data is moved to a country where the legislation is inadequate or it is in contrast to national legislation of the data owner.

NRENs also need to consider potential legal issues associated with cloud services e.g. security breach disclosure laws, privacy requirements, law enforcement issues, international laws and regulatory requirements.

4.5.2 Data protection

Data security, and more precisely protection of personal data, is one of the biggest concerns which greatly influences the uptake of cloud computing. Research and educational institutions need to keep full control over the data, which also includes full responsibility for the data processing.

The treatment of personal data and other sensitive data is regulated by local legislation, and the institutions are already familiar with this issue. However, putting sensitive data in the cloud opens a new area of uncertainty

and questions: who can access the data, how it is stored, processed and deleted, where it is stored etc. There is the requirement to protect data and prevent unauthorised disclosure and loss, but many cloud providers state that they accept no liability for any loss or destruction of data.

4.5.3 Compliance

In moving business processes and data to a cloud, certain obligations and responsibilities are transferred to the cloud provider. If the user institutions are required to meet some specific compliance requirements (such as ISO 27000) the cloud provider must also be part of that compliance process. Otherwise, the institutions are exposed to the risk of breaching existing policies and becoming non-compliant.

4.6 Environmental influences

Using cloud services instead of local infrastructure and provisioning obviously lowers the power consumption from the user perspective. In fact, the power consumption is moved to the cloud provider side. But larger data centres such as those used by major cloud service providers are generally more efficient than local datacentres or small computer rooms. Efficiencies are achieved by resource sharing using virtualization, with higher and more balanced usage and more economical cooling. Therefore, it is widely accepted that cloud computing reduces the energy consumption and positively influences the environment and in particular the overall carbon footprint.

5 Internal influences

Despite the variety of organizational models and the fact that the NRENs are operating in different countries, they share a number of common internal similarities. These internal characteristics influence the NREN's opportunities to be an active partner in cloud services provisioning. The most important internal characteristics of NRENs are emphasised below. These factors need to be taken into consideration as unique internal strengths, which may help NRENs develop their cloud strategy.

5.1 Nationwide network operator for research and education

In most European countries, NRENs have built and continue to operate nationwide backbone network and pan-European and Internet connectivity through the GÉANT network. Those backbones have evolved from a novelty to an indispensable infrastructure for research and education. Providing this infrastructure has earned NRENs high levels of trust by their respective constituencies, and sustainable structures for governance and financing are often in place.

The NRENs are natural focal points for services to their clients due to the network footprint and associated services layered on top, combined with the organisation ethos i.e. focus on education and research as well as close relationships with end user institutions.

Research and academic institutions are faced with cloud computing as a dynamic new paradigm with high potential, but also high levels of uncertainty: technology change, risks of vendor lock-in, legal/regulatory risks and so on. NRENs are well placed to help these institutions navigate the uncertainties jointly and based on established long-term relationships and trust.

5.2 Local infrastructure capabilities

The provision of a high quality secure managed network is typically complemented by local NREN datacentres and local storage which is an ideal basis upon which to layer cloud services. The NRENs are therefore in a strong position from a technical infrastructure perspective to act as a national hub for cloud services by aggregating demand from the existing client base with whom technical connectivity is already in place as well as contractual relationships. NRENs could respond to these demands by using the appropriate cloud service and deployment models.

There are a number of benefits which may support the NREN being a national hub also for providing cloud services in the education and research sector including:

- Dedicated community focused high performance network with high availability
- Non-profit focus compared to commercial organisations, with the intention of offering bespoke services based on community's need
- Community focus and understanding of the NREN, research and education areas
- Potential to offer simpler pricing models compared to public service providers

5.3 Identity Federation services

The identity federation capability provided to clients represents additional added value which NRENs can offer to enhance security and ease the burden of administration through the benefits of Single Sign-On (SSO). Where NRENs are providing direct cloud services e.g. IaaS, local storage can also be attractive to clients whereby data protection concerns are met by keeping data within national and community boundaries and infrastructure accessible for compliance audits.

In the case of brokered cloud services, there are not too many institutions in the sector that have the scale, and are as well respected and competent as the NRENs to negotiate integration of identity federation with commercial cloud providers. NRENs are therefore in an ideal position to represent the interests of the Education and Research community and aggregate demand to get a better technical and commercial solution for clients. The brokered service may still benefit from being federated or directly peered and may even be hosted in the NREN datacentre for a dedicated community service.

5.4 Staff capabilities

From the beginning, NRENs have typically been pioneers in adopting state-of-the-art technologies and this requires highly professional staff with a wide range of knowledge, skills and expertise. This is especially true in technical areas, which in the case of NRENs primarily covers network infrastructure and services, but also security, system administration and software development. NRENs are already serving the research and education community and understand its needs and demands. For that reason, the uptake of cloud computing as a new emerging paradigm is a natural process and new challenge for NREN staff to extend the services portfolio. Not only this pool of competent staff will give NRENs the unique capability of acting as a broker on behalf of their community, but also it can empower them in defining the technical needs of ensuring a successful cloud implementation and monitoring the services offered in case of adopting the managed cloud or the virtual cloud as a solution (see Figure 3).

A cloud service would be just another service in the NREN portfolio where the whole lifecycle needs to be covered by professional support. For that reason, other non-technical skills are also important for successful adoption of cloud computing in the wider community. Most NRENs already have these non-technical skills which have been developed to bring NREN products from solution to service level, such as service management and operation, procurement, legal, marketing, help-desk support etc. Nevertheless, it is worth emphasizing that most NRENs, if not all, don't have expertise to develop, build and provide 24x7 support for the in-house cloud services. This can severely influence their decision in choosing the in-house community cloud as an ultimate solution.

The NREN should carefully consider whether it has sufficient resources with the right skillsets to develop, implement and operate a cloud service(s). In the face of lack of suitable resources and possibly in an uncertain environment where the technology and in many cases NREN client is not yet mature, it may be useful to consider the brokerage approach with a cloud provider (described in section 6.3), and use the resources and possibly even the infrastructure to provide a cloud service.

5.5 Community non-profit ethos focused on the education and research sector

In delivering highly professional ICT services to end users, NRENs have established a trust relationship with the community based on their non-profit ethos. This unique position does not appear in the commercial environment, although many commercial cloud providers offer free but limited services. Therefore, it should be used to facilitate the introduction of new valued services, like cloud computing. Those trust relationships can, in some cases, be manifested in existing services, like AAI (Authentication and Authorization Infrastructure) that should be used in new cloud services as an added value.

6 Cloud strategy formation

6.1 Towards cloud solutions

Based on the comprehensive set of information, collected and analysed during the strategic analysis process, the next step in cloud strategy formation is to setup strategic goals, which reflect the NREN vision with regard to user demands. Different business cases, solutions and implementation scenarios need to be investigated to test if the goals are realistic, feasible and achievable, and therefore if it is worth investing in. It is an iterative process of strategic thinking with feedback loops where some solutions and options can be, and most probably will be discarded, while new ideas and possibilities will appear. At the end, one or just a few most preferred solutions should be identified as the best opportunity for cloud deployment with maximum advantages in a cost effective way.

Settings the goals and making strategic decisions needs to be aligned with the NREN vision and existing strategy or with other policy documents, such as constitutional acts, bylaws, management and operational principles. This policy environment differs for many NRENs, but there are a number of initial questions in the context of cloud computing that each NREN should ask itself in order to drive the strategic thinking:

- What does the NREN expect of itself?
- What do others (users, funding bodies, wide community) expect the NREN to do?
- What is the NREN hoping to accomplish?
- What does the NREN need to do to move toward and achieve its goals?

There are many answers to the above questions and therefore many possibilities to further develop the cloud strategy. This strategy development needs to be based on the inputs from previously performed analysis and driven by user demands and business cases rather than technical challenges. The specific results of this process are the choices and decisions made on the basis of the following key questions:

- Which user community is targeted - ordinary researchers, “long tail of sciences” researchers, teachers, students etc.?
- Which user needs should be addressed - commodity computing or high performance computing, storage or backup service, collaboration and productivity tools, eLearning, file sharing etc.?
- Which cloud service model(s) to choose – SaaS, PaaS, IaaS or some other?

There is a wide range of combinations of the above possibilities and all are focused on which cloud service to provide for NREN user community. Once the cloud service is selected, the next focus of the strategic thinking process is how to provide the cloud service, with two essential questions in defining the NREN cloud solution:

- Which cloud deployment model to implement or support – Public cloud, Private cloud, Community cloud or Hybrid cloud?
- What will be the role of commercial cloud providers in cloud service provisioning?

Answering these questions finally leads the NREN to the central point of the cloud strategy:

- What will be the NREN role in the cloud provisioning?

The rest of the section further discusses these topics that will shape the NREN cloud solution.

6.2 Cloud deployment models

The NIST has defined four cloud deployment models, which are widely accepted in the literature and industry practices:

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

These four models are briefly explained below, addressing the possibilities for NRENs to implement cloud solution for the user community.

6.2.1 Public cloud

Public cloud infrastructure is made available to the general public and is owned by an organization selling cloud services, e.g. commercial cloud provider. A wide range of public cloud services have been already extensively adopted by clients, including NRENs' community (Gmail, Office365, Salesforce, Amazon Web Services - AWS, HP Cloud, Dropbox etc.). Many of these cloud services are offered for free with limited capacity or functionality, which is often enough for individual usage. At the institutional level the commercial usage of public cloud services is becoming popular in the research and education community.

Bearing this in mind, there is still room for NRENs to help their users by acting as a cloud brokerage and provide the cloud services for lower commercial prices and better contractual conditions, adding additional value though integration e.g. with AAI federation.

6.2.2 Private and Community Cloud

NRENs may wish to consider using private clouds for internal use e.g. for internal IT usage or as a computing platform for delivering services to its clients. Going beyond the internal private cloud, a strategic goal for most NRENs will be to offer or support a cloud service to its own community e.g. IaaS Storage or Compute (VMs) or indeed SaaS services such as a Moodle VLE service.

The platform for private cloud is typically quite similar to community cloud e.g. OpenStack, VMware vCloud but providing a community service will add extra requirements such as:

- supporting a multitenant environment
- security requirements to segregate and protect different client environments
- billing/charging functionality and pricing models
- data protection considerations e.g. data privacy, backups, archiving of client data
- need to integrate with a client environments at a network or application level
- service requirements of clients e.g. SLAs, Service Management Resources
- support for AAI

The private or community cloud could be built and supported using NREN resources and in the NREN datacentres or using the services and possibly the infrastructure of an external vendor (see cloud provider model in Figure 3). It should be noted that depending on the nature of the service and technology, building an

own private or community cloud and providing it as a production service to clients can be a significant challenge for an NREN in terms of financial cost and/or manpower. However, having precise analysis and knowledge about the community needs and demands can lead to the successful case studies (Appendix A).

6.2.3 Hybrid cloud

The Hybrid cloud model could be an extension of the Private/Community cloud model whereby resources and services available in public cloud(s) can be used in a complementary fashion. An example of this is where compute resources in the NREN private/community cloud can be supplemented by those from a public cloud at particularly busy or peak times. The use of elastic cloud resources could be of interest for short but intensive scientific computations in combination with commodity usage of other users. This requires applications to support this type of elastic capability but provides maximum flexibility for NRENs and their clients. The adoption of the Hybrid cloud approach although currently immature is predicted by vendors and industry analysts to become a major trend in IT over the coming years.

6.3 Dealing with commercial cloud providers

Commercial providers have always been a necessity for many NRENs in delivering services, and they need to be considered as one of the most recent developments. The range and depth of options for commercial cloud services is significant and evolving rapidly with major implications for NRENs and their clients, including where and from whom they receive the services.

In developing a cloud strategy, it is important for NRENs to coordinate activities and to work on the basis of a "rules of engagement" consistent with the mandate, ethos and vision of NRENs which may vary from country to country, but in general can be summarised by the following principles:

- NRENs should not seek to directly compete with commercial providers in the provision of cloud services. NRENs should consider providing cloud services directly to clients where they can provide a clear added value e.g. services which are not available commercially or where the NREN can provide a differentiated service e.g. leveraging the benefits of the NREN networks, utilising higher performance networks with managed end to end capability, cost advantages, federated access etc.
- NRENs should not seek to profit from the reselling of commercial provider services. NRENs should seek only to cover costs incurred in the negotiation of any commercial agreements and pass on the cost benefits to its clients.
- Engagement with commercial providers should be done on behalf of clients to optimise the commercial benefits and offered service levels. This could include for example aggregating client demand on a national or international basis (co-operating with other NRENs) to provide the best commercial and contractual arrangements representing the needs and interests of clients.

The above points are of course subject to the ethos, institutional strategy and vision, as well as operating realities of each individual NREN. In general, the guidance for dealing with commercial providers should be based on maximising the benefit of the core asset i.e. the network for the benefit of NREN clients and their business requirements.

6.4 NREN role in cloud provisioning

Cloud services are in general highly complex and bespoke and require significant organisations for development and support activities. While many of the building blocks of such services are well known and often core skillsets to NRENs, the additional layers of functionality, such as elasticity, self-service, on demand usage and billing, bring new challenges to NRENs. While many NRENs have the skillsets to develop cloud services and support them in a production environment, for many NRENs this is not feasible.

Bearing in mind the above, the NREN's role and engagement in cloud service provisioning converges to one or more of the following options:

- Cloud neutral
- Peering with commercial cloud providers
- Cloud brokerage
- Cloud provider
- Multi-layered approach

These options and cloud deployment models are elaborated on further in the text below.

6.4.1 Cloud neutral

NRENs and their clients are likely to require a variety of cloud services from multiple providers i.e. it is not likely to be a one-size-fits-all approach to cloud services. The issue is discussed in more detail in the multi-layered approach model. Bearing in mind this multi-cloud, multi-vendor environment and likelihood that public or external services are already being deployed, there is a risk that, if nothing is done, users will drift into fragmented islands of incompatible services that may not have a sustainable future. Doing nothing carries the risk that, in the long run, cloud operators turn the network infrastructure into an irrelevant commodity, effectively replacing a high performance and quality network by simple commodity connectivity, limiting the future educational and research activities at the most basic infrastructural level. If the NREN strategic decision is to stay away from cloud service provisioning for the community, it is recommended that the NREN also takes a neutral stance towards individual vendors and technologies and encourage the support of common interoperability standards.

6.4.2 Peering with commercial cloud providers

In many cases NREN clients are already using public commercial cloud services (e.g. Gmail, AWS, Blackboard) and the NREN network plays a critical role in the delivery of these cloud services to end clients. If the NREN strategic choice is to stay in its traditional core business and well-known area – the network, another option to support client community is to improve external cloud services by peering directly with the cloud providers. It would keep the external cloud service on the managed NREN network rather than the unmanaged general Internet traversing multiple service providers. Peering maximises the benefits for NREN clients by improving service levels and reducing risk. It maximises the benefit of the NREN network for clients and therefore in general should be seen as a positive contribution.

Current cloud public services normally charge for network traffic to its users. In this context global connectivity agreements by the NRENs at European level are desirable, to lower prices of network traffic of cloud computing services to NREN users. Also advanced network services, like IPv6, should be promoted.

6.4.3 Cloud brokerage

Another level of NRENs engagement in cloud service provisioning for client community is to act as a *broker* for third-party cloud services towards its constituency. It means that the NREN does not deliver cloud services directly to its users as a provider, but instead organizes, promotes or manages public or external services from the commercial service providers existing on the global market or indeed from other NREN organisations.

Most NRENs have already been doing brokerage for their clients - working with suppliers to get the best commercial deal by aggregating demand. The role of a cloud broker allows an NREN to bundle its community's specific requirements as well as buying power to negotiate attractive deals from leading suppliers. Specifically NREN should spend effort in aggregating demand, cloud brokering and vendor management. By brokering solutions for its client base, the NREN can achieve economies of scale (by combining national and possibly international demand) compared to individual institutions but also substantially remove the overhead associated with on-boarding new service providers and the procurement effort, technical due diligence etc.

NRENs should take the lead in the field of cloud brokering and cloud middleware infrastructures, and be able to connect the clouds and provide added value to their members. Reusing existing cloud middleware infrastructures, like AAI, are clear benefits for the user community, so this objective should be pursued by NRENs. These infrastructures are related to the unique user identity on the network, and should be availed on the services, including cloud services. Therefore, cloud services should be compatible with the existing AAI federation.

Brokering cloud service offerings should bring clear information to the user, about updated and reliable service descriptions and service levels. Where possible a legal framework for public acquisitions should be made available to NREN users, tailored to the specific community requirements. These objectives lead to an unavoidable vendor management requirement and coordination that should also be availed of to promote inter-operability requirements between different public clouds. Interoperability is essential to mitigate vendor lock-in traps, when the user is forced to use services with degraded quality or increasing, non-competitive, prices.

In practice, however, there are some limitations: leading suppliers already know how to sell to enterprises and don't like additional middlemen, although competing suppliers may be grateful for help entering the market. For some NRENs, the loss-of-control concerns cannot realistically be resolved by introducing a broker.

6.4.4 Cloud provider

In cases where NRENs wish to provide their own cloud service for their user community and not for example broker an existing service with a commercial vendor, NRENs are challenged to become a cloud provider, providing community cloud for the clients. There are many possibilities for NRENs to deliver their own cloud services and third party cloud providers (commercial providers or other NRENs) can still play a significant role. Moreover, the options to deliver NREN cloud service are determined by the roles and responsibilities of these two main actors – the NREN itself and a third party cloud provider, relating to the following key issues in cloud service deployment:

- **Ownership** – who owns the cloud infrastructure, which includes physical assets, licences, supporting hardware etc.?
- **Management** – who is responsible for cloud infrastructure governance, operations, monitoring, security provisioning, compliances etc.?
- **Location** – is the cloud infrastructure located on the NREN data centre (on-premises) or under responsibilities of the commercial provider (off-premises)?

These three dimensions on how the roles and responsibilities are shared between NREN and the third party cloud provider are depicted by the following cube model shown in the following figure.

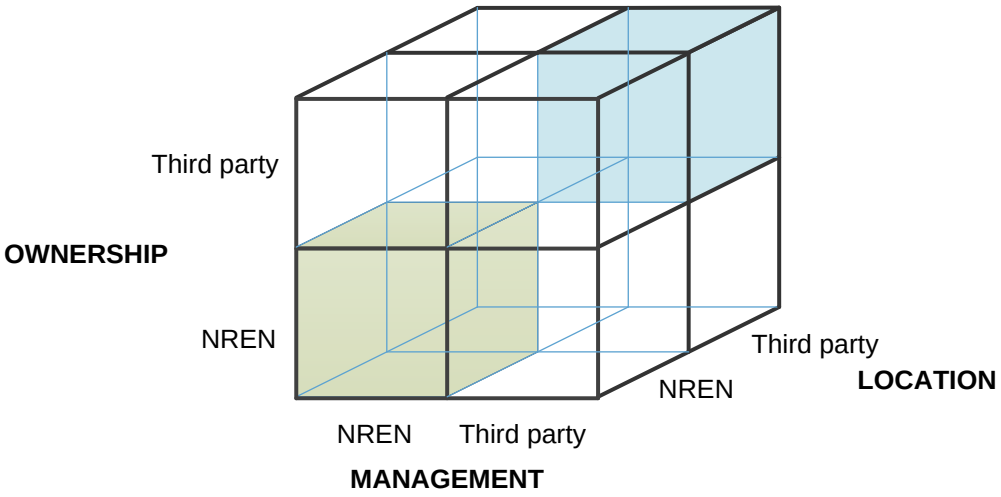
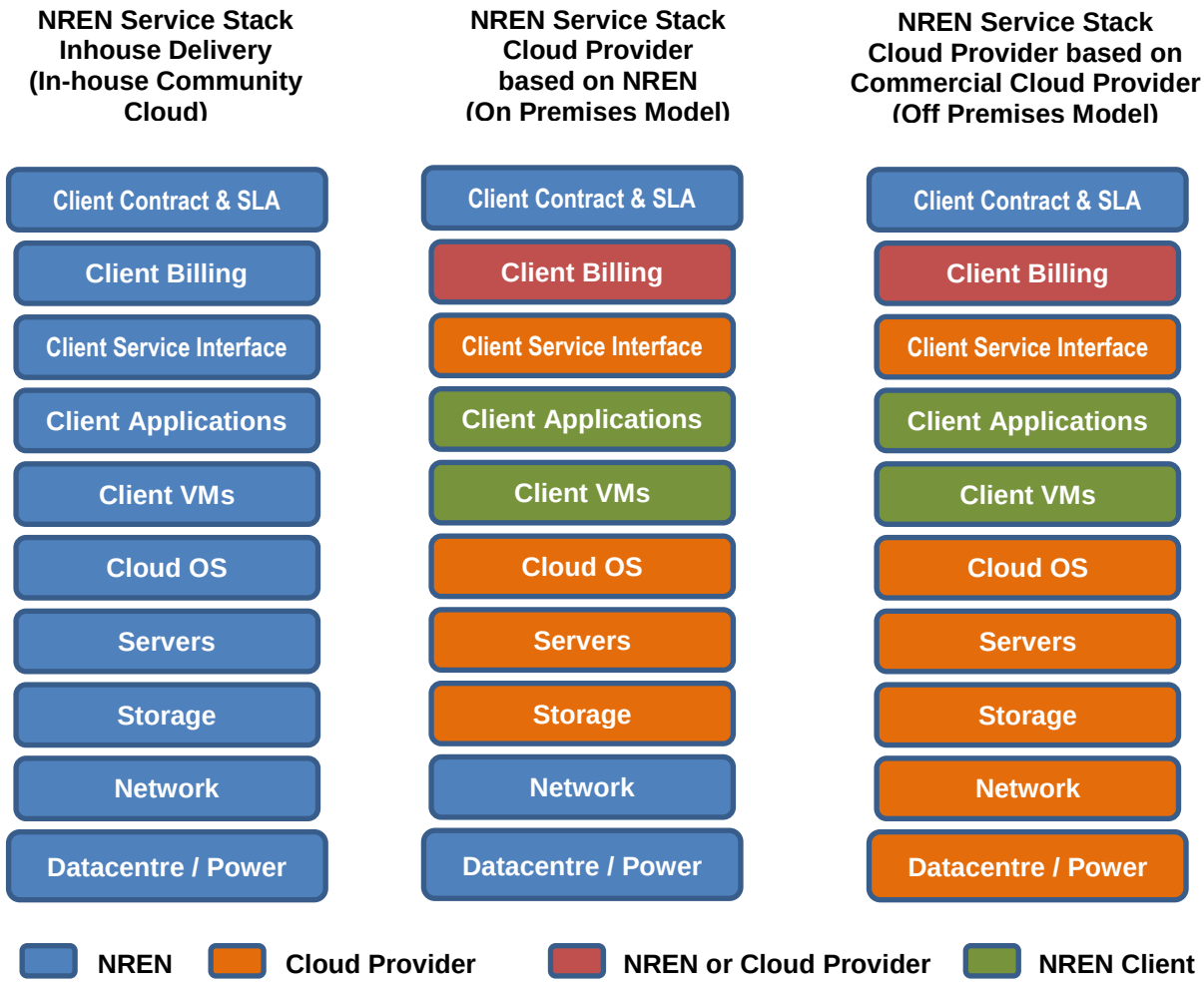


Figure 2: Roles and responsibilities: options for sharing between NREN and Cloud Provider

In the extreme case (bottom-left-front corner), the NREN cloud service is fully in-house, delivered and provided through a private/community cloud developed and managed by the NREN itself, running on the NREN own equipment and premises. On the other extreme of the spectrum (top-right-back corner), the NREN cloud service is fully outsourced to a third party provider, who builds and manages the cloud service on its own infrastructure and datacentre.

A realistic approach to consider is to use a commercial cloud provider to deliver a dedicated managed service. In this case the NREN can use a commercial cloud provider to provide the resources and expertise to build and operate a cloud service for its end user clients but with the service still being an NREN service. With this approach the NREN is managing the cloud provider who is effectively providing a managed service. The advantages of this approach are that the NREN is in a position to provide a new service without having to invest in building up in-house dedicated technical resources. This could potentially speed up the process of launching new services by avoiding the time, cost and effort of building specialised teams by using teams already well-established and experienced in a commercial cloud provider. The approach also reduces the financial risk as it could minimise the financial commitment by the NREN e.g. where there is uncertainty about the viability of a potential cloud service. There are also potential disadvantages with this approach as there is a risk of vendor lock-in as well as increased dependency on a commercial vendor and their ability and commitment to continuing to provide the managed service at a competitive cost. HEAnet in Ireland have used this model successfully to provide its Storage as a Service solution (Edustorage) whereby the HEAnet service is supported by an external company (IBM) (Appendix A.1).

Since a cloud environment is based on multi-layered infrastructure, the roles and responsibilities of cloud infrastructure management in the above cloud provider model can be subdivided and shared across the layers of the cloud stack – from a physical hardware, virtualization platform, up to an application level. Figure 3 below provides a broad comparison between the varying approach from the NREN taking full ownership and management of the entire service stack to using the services of a cloud provider either on premises or off premises.



The use of third party cloud providers will depend on the requirements of the NREN and this may evolve over time as the NREN requirements may change. This approach could be used as a short to medium term strategic option for NRENs to launch a cloud service(s) where resources and skillsets and experience are limited as well as a mechanism to mitigate risk in the face of uncertain client demands or technology risk. The degree of dependency on an external cloud provider could be varied over time e.g. reduced as the NREN builds up its own capability. It is worth mentioning that in all cases with the cloud provider model, the cloud service delivered is always under the NREN's branding and service portfolio.

6.4.5 Multi-layered approach

NREN client's IT requirements are likely to require a variety of cloud solutions to deliver services in the future and will avail of cloud based services to an increasing degree which in many cases will replace traditional campus IT.

It is likely that no one solution or vendor will provide all the answers to client requirements – the future landscape is likely to consist of traditional on-campus IT for critical, sensitive or bespoke applications and services as well as Private, Community (NREN based) and Public cloud solutions. A University might for example use Public cloud SaaS solutions for student email and virtual learning, traditional IT for ERP, an NREN IaaS Community cloud to host low to medium priority applications on VMs and Public cloud for low priority and low sensitivity applications and storage. This "multi-cloud" environment will likely require a multi-layered approach and NRENs may need to consider a variety of activities as described below to best serve their clients including:

- Peering with major service providers e.g. Google, Amazon, Microsoft, Blackboard to maximise the performance and service levels by keeping the user traffic on NREN managed networks rather than the Internet
- Broker Services (Cloud Service Brokerage) – with commercial vendors and other NRENs
    - Contractual agreements to aggregate demand for the best commercial deals
    - Contractual and technical e.g. Technical due diligence, AAI Federation
    - Cloud Provider solutions to provide a dedicated service to NREN clients using either the on-premises or off-premises models outlined in the previous section
- The NREN builds its own cloud services e.g. IaaS Cloud Compute only where the NREN can provide a higher grade or differentiated service, or no suitable service is available commercially or where legal or government directives apply e.g. restrictions on data location.

The above multi-layered approach is not new for most NRENs, and requirements will vary from country to country reflecting the reality that it will not be a "one cloud suits all" future and clients will choose the best option (provider) for each service with an "a la carte approach".

7 Implementation Issues

7.1 Roadmap development

To ensure that the cloud strategy is successful, a roadmap is needed to define the major activities and resources needed to achieve the strategic goals with acceptable cost, time and efforts.

If the NREN goal is to provide or support a cloud service to the client community, the roadmap would consist of the following three phases:

- Preparation phase – includes activities to prepare the project team, establish budget and procurement, as well as technical activities to specify technical requirements, acceptance criteria, and design the service with all necessary details to achieve the specification.
- Implementation phase – the activities needed to bring the service live, which includes conducting the procurement, technical installation, configuration, testing and onboarding, as well as supporting activities, such as project management.
- Operation phase – long term activities that include day to day service operation, monitoring, reporting, maintenance, support, helpdesk, training, promotion marketing etc.

These phases and activities are generally given at a high level, but they can be applied (with appropriate modification) to any previously mentioned model. In the case of a cloud provider model, the activities are shared between the NREN and the third party cloud provider according to their roles in a cloud service provisioning.

As an example, Figure 4 and the text below describes each phase with major activities for establishing a NREN cloud service provided and managed by the commercial cloud provider.

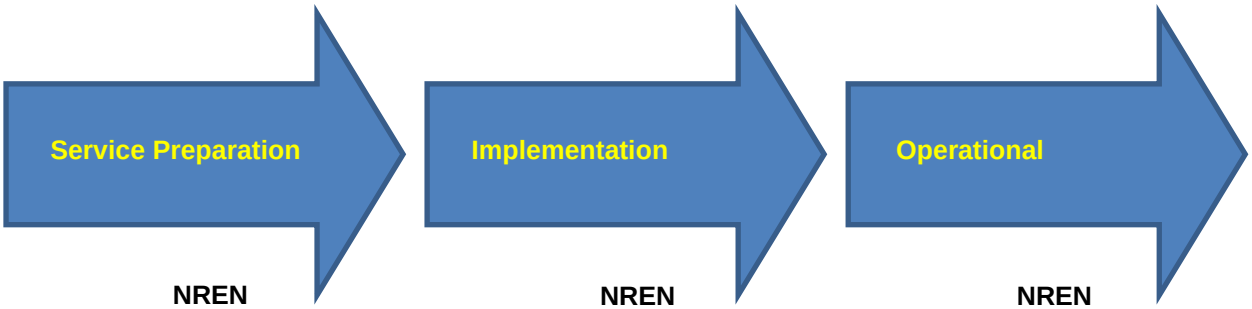
Service Preparation Phase - In this phase the NREN must define the characteristics i.e. the functional specifications of the service it wishes to design and offer its client organisations. The Service design is likely to be based on the outcome of the NREN's Cloud Strategy and a Feasibility study to define the types of services which are attractive to clients as well as resources and skillsets required and the business case. As an example, the functional specification of the Cloud service for an IaaS service offering virtual machines may include following items:

- types of VMs to be offered – sizes, operating systems supported
- storage options e.g. block storage, object storage, backup capabilities, snapshotting, encryption
- high availability requirements e.g. live migration of VMs across datacentres
- support for API access for client organisation
- self-service portal features e.g. role based access control, federation, diagnostic capabilities, compliance reporting
- billing model e.g. usage based, free, external interfaces to billing systems
- SLA requirements e.g. availability, data durability, reporting, response times, hours of support
- Requirement to use or interface with existing NREN infrastructure and services e.g. storage, billing or green field approach – in NREN footprint or in cloud provider
- Service delivery e.g. Cloud provider will build cloud and NREN will operate it or cloud provider will operate service for the NREN as a managed service either in NREN datacentres or in cloud provider datacentres

If an NREN is adopting the Cloud provider model a significant procurement exercise will be required to select a cloud provider based on the specifications of the service. The Cloud provider will need to design a solution based on the specifications defined by the NREN. The NREN may benefit from a technical dialogue approach to the procurement, to gain an in-depth understanding of the different cloud providers in the marketplace and their capabilities to help refine the details of the functional specification which will typically be documented in an RFT (Request for Tender) as part of the formal procurement process.

Implementation Phase - During the implementation phase the NREN will need to manage the cloud provider to ensure it delivers the solution required as specified in the solution design from the previous Service Preparation Phase. The NREN will need to define its Acceptance Criteria and ensure that the cloud provider builds the solution and validates it e.g. through User Acceptance Testing (UAT). During this phase the NREN will be acting as a project manager of the cloud provider and also maintaining ownership of the relationship with the service users which may require managing the process of onboarding client organisations e.g. setting up SLA agreements, training, pilots etc.

Operational Phase - Once the cloud service is built, the NREN focus will transition to issues of a day to day operational nature e.g. managing user requests, service outages, service reporting, updates etc. If a cloud provider is being used for service delivery during the operational phase then the NREN will need to manage the service delivery by the cloud provider e.g. ensuring the cloud provider meets service Key Performance Indicators (KPIs) in the delivery of the service. The NREN would typically maintain ownership of the relationship and contract with the end user organisation. The customer interface at an operational level e.g. billing, service desk may be provided by either the NREN or the Cloud provider depending on the agreed service design.



NREN
- Functional specification
- Procurement

Cloud Provider
- Solution Design

NREN
- User Acceptance Testing
- End user organisation onboarding
- Project management

Cloud Provider
- Detailed technical design
- Configuration
- Testing
- Project management

NREN
- Vendor Service Management
- End user service management

Cloud Provider
- Operational support

7.2 Security

Cloud computing presents many important security challenges that while challenging are well known. The Cloud Security Alliance (CSA) has identified 14 domains (see figure below) to be addressed as a part of security policy and management, but the treatment of these security challenges depends on the role organizations have in cloud provision and the usage model. NREN clients, i.e. the research and education organizations, have a user-centric view of security issues that need to be provided and guaranteed.

The opposite viewpoint of security issues compared to the user centric view above is from the role of cloud provider as the service provider to NREN clients, who needs to provide appropriate policy and control mechanisms to ensure high levels of security. When implementing and offering cloud services to its user community, the role of the NREN may be either of these two viewpoints depending on the deployment model chosen. The security issues to be considered by NRENs are not only relevant in the direct provision of own cloud services (in-house deployed or outsourced managed services) but also when the NREN acts as a broker of cloud services as there will still be legal and contractual requirements which the NREN will need to put in place with the service provider. Therefore, the NREN role in solving security challenges in cloud strategy is

more complex and includes understanding user expectations as well as provider obligations regarding a wide range of security issues (some or all of the 14 domains identified by the CSA). It is important to make a demarcation border between all three actors, i.e. user organizations, NREN and commercial provider (if it is involved), and strictly define security management domains, for each role and the corresponding responsibilities.

This demarcation border for the user organizations depends on the chosen cloud service model. In the case of IaaS the users have most control over the resources and responsibility for the security of the cloud stack, from the level of virtual machines up to the applications. Going further up the cloud stack, when using PaaS and especially SaaS, users have less control and hence have to rely more on the cloud provider to implement sufficient security mechanisms. In reality, commercial cloud providers often give little or no information about their security practices, except general security policy statements.

The NREN involvement in this process depends on the deployment model and, more specifically, depends on the NREN role in this model which may be providing own cloud services based on NREN on premises infrastructure, offering cloud services managed by an external outsourced company or acting as a broker of cloud services delivered by a commercial provider.

Concerning security issues, in all cases the NREN must work in the best interests of the user in order to provide well-defined security management and clear assurance or at least to clarify security concerns. The more security questions that are identified early to identify risks, the more these risks can be analysed and resolved in the early phase during the strategy formation and implementation planning and the less problems are likely to arise later during the operation and usage phase.

Regardless of the NREN role in cloud service provisioning, the rest of the section lists some of the issues and questions that need to be addressed, analysed and clarified from the position of the NREN client organizations and the NREN itself. These issues cover all layers of the cloud service stack and need to be put in context for the entity that does provide this part of the stack – whether the NREN or a commercial cloud provider.

7.2.1 Physical security

- Physical access – what policies or procedures are applied to access the physical equipment and communication infrastructure or network, what relevant security standards are in place (e.g. ISO 27001), how is physical access protected, what kind of monitoring and controls of physical security is applied, is there an electronic surveillance system, security cards and alarms in place to prevent unauthorized access, who other than IT staff can access the IT infrastructure.
- Asset management – is the automated inventory mechanism applied to keep the list of physical items up to date, are assets classified in terms of security and criticality, what is the mechanism to avoid the backdoor left in the system.
- Equipment installation/removal - what policies or procedures are in place for loading, installing and removing equipment, how are the suppliers and subcontractors managed against possible security threats, how are equipment and old media with user data destroyed.

7.2.2 Network security

- Protection against remote attacks – what kind of firewall protection is in use, which mechanisms are used to mitigate DDoS attacks, is deep packet inspection used, what defences protect against internal and external attackers, what level of isolation is supported by the network architecture (VPNs, VLANs), with whom is L2 network connectivity shared and how is it protected against L2 attacks (for instance MAC spoofing and ARP poisoning).
- Configuration and change management – what policies or principles are in place to provide smooth and secure changes in network architecture, how is network configuration management organized, are the configurations versioned, are the configurations backed up to a secure location, who can access the configurations, are internal cloud network management segments isolated from the production network(s).
- Data confidentiality and integrity – how is user data secured in terms of confidentiality and integrity in transit through the network on the path from user organizations to cloud provider, including transfer through NREN and GÉANT network.

7.2.3 Host security

The responsibilities for host security depend on the cloud service model in use. In the case of PaaS and SaaS the responsibilities are transferred to the cloud provider who is responsible for all layers up to the application platform, while in the case of IaaS the user is primarily responsible to provide host security for virtual instances and guest operating systems.

Questions of concern for the user that need to be raised with the cloud provider are: what is the level of protection of virtual images by default, is the principle of least privilege provided, is the host firewall system configured with minimum ports opened to support services running, is there any intrusion detection system running on the host, what is the protection from unauthorized access and login, is there a monitoring and alarming response for unauthorized login attempts, what backup and recovery systems are in place.

7.2.4 Application security

Similar to host security, responsibility for application security is also shared between the cloud provider and cloud customers, e.g. NREN clients. Application security for the SaaS model is entirely under the responsibility of the cloud provider. In the case of PaaS the cloud provider is responsible for the security of the application platform, while NREN clients are responsible for the applications deployed on the platform. For IaaS the responsibility for application security rests entirely at the NREN client level. Noteworthy, even for models like Paas and IaaS, involving a high degree of responsibility on users' side, the cloud provider is still liable to ensure that activity or carelessness of some user will not adversely affect other users. For example, mis-configuration of virtual network elements resulting in ARP storms, failure to apply security patches to a webserver resulting in the machine being compromised and becoming a distributor of malicious or copyrighted content. Protection against these events should be carefully designed, at the hardware, monitoring, and procedural levels.

Some of the typical user concerns will be: what kind of security features are provided to protect the applications, does the provider regularly run penetration and vulnerability tests, what are the policies or principles for patch

management, what are the policies or procedures for new application release and deployment, how is user data isolated in multi-tenant application environments.

7.2.5 Information security

- Personal data security – what standards, policies or procedures are applied to protect personal data, under which legislation is the security of personal data ensured, in which country is data stored (original and backup copy), what kind of personal data is required for registration to use the service, is it possible to export user data in an interoperable format.
- Encryption – are there well-defined policies or principles implemented for data encryption, is data encryption provided by the cloud provider (by default or optionally), what data is encrypted, where is the encryption used – in data transit, storage or memory, what kind of encryption algorithms are used, what is the key length, is proper key management established, how are the keys secured, who holds and can access encryption keys, are procedures in place in case of a key being compromised, can the user additionally provide her own data encryption, is the system audited and compliant with industry standards.

7.2.6 Personnel security

Individuals are often the weakest point in the security supply chain. This raises questions such as: who has rights to physically access data centres and equipment and permissions to access user data, how the personnel are screened when the company is hiring staff, how are information security responsibilities assigned to staff, do IT and other staff have the required security education and training, what procedures and roles are in place to grant, review and remove access rights.

7.2.7 Identity and access management

With an essential cloud characteristic being the ability to provide easy access from anywhere, identity and access management is one of the top issues in provisioning secure cloud service operation. NREN clients need to be assured that well-defined policies are in place and proper controls have been implemented to protect user service and data from unauthorised access both externally from anyone and anywhere as well as internally from unauthorised internal staff. Additionally, NREN clients could demand mechanisms to manage their own users' access within cloud service.

- Identity management - is it possible to integrate a federated identity management infrastructure into the cloud service, is the identity and access infrastructure interoperable with other identity providers, is there a possibility to implement single sign-on, what checks are made on the identity of user credentials at the registration process.
- Authentication – what credentials and authentication level is required/supported (e.g. username/password or two factor authentication with one time password and token), what are the requirements for password strength (length and difficulty), what mechanisms are in place to protect attempts of unauthorised access, how these attempts are logged and inspected, can NREN clients have access to audit logs, what is the procedure if user credentials are compromised.

- Authorisation - what are the principles for allowing and approving accounts with system-wide permissions, what is the access policy for those accounts with highest privileges - especially for remote access, is the principle of least privileges applied to grant users with minimal privileges only to access the system resources and data they need to, is there a procedure in place to regularly audit authorisation methods to ensure compliance to industry standards.

7.2.8 Incident management

In addition to the above mentioned security issues and areas of concerns, security provisioning and operation also covers the following topics that address efficient incident detection in a timely manner and the appropriate reaction to minimise the impact of the incident.

- Incident prevention – what policies, procedures or measures are in place to assess security risks and prevent security incidents throughout the service stack, how often are these reviewed, is there dedicated staff to apply these security policies, procedures or measures, are these regularly audited to ensure compliance and detect security breaches (penetration tests, vulnerability tests).
- Security monitoring, detection and analysis - what procedures and principles for security monitoring are in place, is real time monitoring in place, what mechanisms are applied to provide audit logs of security related events, what kind of events are logged, for what period are these logs kept, who analyses and processes these event logs and how can NREN clients have the appropriate level of access to logs, and if so how is the log data relevant to other clients isolated, what method is used to provide the integrity of event logs, what controls are used to protect systems against malicious codes.
- Incident response and recovery - what procedures are in place to respond in the event of service disruption, what are the possible impacts to clients in the event of an incident including recovery actions, how are incidents documented and reported to NREN clients, are all incidents regularly reported, what is the method to notify and report to NREN clients (e.g. public announcement on the web site, email to client or upon client demand).

7.2.9 Business continuity

NREN clients are always looking for the highest service quality in terms of availability, reliability and performance. In reality, a service could be compromised by security incidents, planned downtime for maintenance or other disruptions caused by unplanned breaks (power supply, air-conditioning, network etc.).

To provide business continuity for NREN clients and maximise service availability, reliability and performance, the following issues are of particular concern:

- Business continuity provisioning – what kind of redundancy is provided for physical infrastructure and resources (power supply, air-conditioning, network, hardware components etc.), what methods are implemented to protect the services from environmental disaster and damage (fire, earthquake, flood, etc.), what procedures and channels are in place to report or announce service disruption, are there well defined procedures with defined roles and responsibilities in the event of service disruption, are there priority categories for service recovery and how the services and clients are categorised in that case, how the security related issues are addressed in the event of disaster.

- SLA – what service quality and features are included in the SLA, what parameters (availability, performances) and thresholds are included in SLA monitoring, are planned downtime for maintenance included in the SLA, are security breaches included in the SLA, is there compensation for the client if the SLA is compromised and how is it achieved, what reporting must be provided to clients.

7.2.10 Legal and compliance

A well-defined legal framework is always necessary for successful strategy implementation, especially when it comes to security in cloud computing. The legal and contractual obligations in service provisioning which govern the protection of client information and in particular personal data will be mandatory requirements. Whenever possible an NREN cloud strategy should show how the service addresses specific requirements of National and European regulations, providing, in that way, clear assurance to the NREN's clients about the service.

The typical issues to be resolved are the following, to ensure that the appropriate legal and regulatory frameworks are in place for all possible stakeholders (user organizations, NREN, commercial cloud resources/service providers and subcontractors): are obligations and responsibilities clearly defined between all involved parties, in what country and jurisdiction area user information is physically stored (including personal data) or accessible from, what data can be subject of access and processing by law enforcement, what is the procedure for making information available to law enforcement and to whom it is allowed, is the user notified in that case, are contracts, user agreements and SLAs negotiable, what are the consequences and limitations of liability in the event of contract breach or termination.

7.3 Risk management

Implementation of a cloud strategy is likely to be challenging due to the potential risks involved regardless to how the plan is well defined and detailed. Risk management is therefore an essential part of the project plan which deals with the undesirable events that might occur and affect the project results, time plan and money. Cloud strategy therefore needs to include proper risk management in order to anticipate possible risks in an early phase, analyse their impact, and plan mitigation approaches. The goal is to minimize the negative impacts of these unwanted events if they occur, take better decisions and, if possible, turn them into opportunities. To do so, the risk management approach needs to identify possible risks and develop corresponding actions that are incorporated into the initial project plan and budget. It is commonly done by conducting the five steps as follows:

- Risk identification
- Qualitative risk analysis
- Risk response planning
- Quantitative risk analysis
- Risk monitoring and control

These essential steps of the risk management process are defined in the text below and are demonstrated through examples of two cloud deployment models – providing brokered cloud service and providing an on-premises based community cloud service.

7.3.1 Risk identification

Risk identification is the first and probably the most important step in risk management. Risks that can affect the implementation of cloud strategy must be identified, understood and analysed including causes and consequences. The risk identification needs to be very specific and put in the context of the cloud strategy, rather than being general describing risks that can happen in every project. Therefore the key sources for risk assessment and identification is the cloud strategy itself and the project plan, which defines cloud deployment activities in more detail.

Each activity, task and decision involves some uncertainty and uncertainty implies risk. The risk can have a knock on effect from one task to other dependent tasks. Therefore, it is also essential to understand any inter-dependence between tasks, especially the critical path through the project plan, and the risk associated with those tasks.

The risk identification process must involve all stakeholders involved in the cloud services deployment defined by the strategy. The most important players are NREN staff that need to conduct the project plan, but also users adopting cloud services, budgets holders supporting the project, cloud providers and vendors who are providing solutions etc.

If the cloud strategy and project plan are not aligned with the NREN organization, especially in terms of the internal strength and capacity to conduct it, there is more likelihood of risk to occur. External factors and changes in them, such as legislation, government, economy etc., can also influence the project plan and the outcome.

The risk estimation and analysis must be part of the cloud strategy from the very beginning, but there will be many uncertainties and changes that are likely to occur throughout the project lifetime. Risk identification is therefore an ongoing process throughout the project implementation rather than one-time activity. General risks concerning any project should be avoided, focusing only on those risks which are specific to the NREN cloud strategy and the chosen cloud deployment solution. Also, a good approach is to involve more people in the risk identification process with a broad range of skills and experience, rather than relying only on the core project team, which will often have a subjective attitude and natural tendency to ignore or underestimate the risks. It is advisable to verify the risk assessment results with other NREN staff who are not directly involved in the project or even external experts.

To be able to manage the risks, a starting point in the risk analysis is to find the root that causes the risk, as well as the consequences to the project if the risk occurs. The risks are described using the *Condition-Cause-Consequence* model:

> "There is the risk that ... caused by … resulting in ..."

For example, in the case where the NREN is acting as a cloud provider implementing a community cloud, a single risk could be described in the following way:

> ***Risk 1: "There is the risk that the service won't be stable enough caused by inexperienced staff resulting in losing users."***

In the case of a cloud brokerage approach, a risk could be identified as follow:

> ***Risk 2: "There is the risk that the cloud provider moves the service to a datacentre in another country caused by its internal decision resulting in a legislation conflict".***

This risk identification log can be extended to a detailed risk register which contains additional fields that are associated to each risk, such as: risk probability, impact, status, mitigation actions (preventing actions, response actions), cost, owner, timescale etc.

7.3.2 Qualitative risk analysis

The register of identified risks that could influence the implementation of the NREN strategy needs to be prioritized by its significance, where more serious risks are on the top of the list. The measure of the risk significance is given by the following factors, which are already identified in the risk register:

- Probability – the probability that the risk will occur
- Impact – the consequences of the risk occurrence, that can be expressed in terms of: Time, Cost, and Quality.

A good approach in estimating the risk severity is to grade the probability and impact from 1 (very low) to 5 (very high), and use their product to express the risk significance, in the range from 1 to 25. Since there is no need for such detailed granularity, these numerical factors need to be categorized into three levels, denoted as red, amber and green, or even only two levels – red and green, using predefined numerical thresholds (for example 10, where green is less than 10, red is equal to or greater than 10).

These risk categories will require different treatment. The red category means that the risk is unacceptable. It means that certain time, money and effort needs to be allocated to a specific response, either to prevent the risk or to promptly handle it if the risk does occur. However, the green category doesn't mean that these risks can be ignored without actions to be taken to prevent and respond to them: instead, it is statistically expected that some of these risks can (and will) occur, but on average they will not dramatically influence the implementation of the strategy.

In the previous example of the risk with the NREN role as a cloud provider, the risk analysis could be extended as follows:

> ***Risk 1: "There is the risk that the service won't be stable enough caused by inexperienced staff resulting in losing users.***

Risk probability is high (4), the impact is high (4). Significance is 16 and the risk category is red (threshold is set to 10).

In the case of the cloud brokerage approach, the risk could be identified as follows:

> ***Risk 2: "There is a risk that the cloud provider moves the service to a datacentre in another country caused by an internal decision resulting in a legislation conflict".***

Risk probability is low (2), the impact is very high (5). Significance is 10 and the risk category is red (threshold is set to 10).

7.3.3 Risk response planning

While green risks are statistically expected to occur, but with no serious damage, risks in the red category are of the major concern and they require a detailed response plan. Depending on the risk classification, appropriate risk responses are as follows:

- Risk avoidance – prevent the risk by redefining the plan in such a way that the circumstances that can cause the risk are removed
- Risk reduction – take action(s) to reduce the risk probability and/or impact
- Risk transfer – moving the risk impact and responsibilities to a third party e.g. insurance
- Risk postponement – lower the risk probability and/or impact by reorganizing the time plan and delaying some activities
- Risk acceptance – accept that the risk can occur and cover the impact if that happened (usually for green risk of low significance)

Cloud provider example:

> ***Risk 1: "There is the risk that the service won't be stable enough caused by unexperienced staff resulting in losing users.***

Risk category is red.

Risk reduction – plan technical training or involve external experts.

Cloud brokerage example:

> ***Risk 2: "There is a risk that the cloud provider moves the service to a datacentre in another country caused by an internal decision and resulting in legislation conflict".***

Risk category is red.

Risk avoidance - Negotiate with the cloud providers at an early stage and implement protection in the contract.

7.3.4 Quantitative risk analysis

Risks may impact negatively in many ways, e.g. in terms of security, performance, client confidence, cost, loss of reputation etc., and therefore the next step in risk management is to quantify the risks e.g. in terms of resources (money, man efforts, time) that need to be allocated in advance to cover the risks and corresponding response actions. Again, red risks are of the most concern, which require detailed resource estimation and planning. It is advisable for the risks which are of high probability and moderate impact to allocate the full cost of the risk rather than scaling the cost based on the probability. In other words if the risk occurs, the full cost is required: otherwise, if the risk does not occur, the allocated budget will be saved. The opposite scenario is for a risk of low probability but very high impact. The cost scaled by the probability means nothing if the risk does occur. Moreover, in this case, the response cost usually exceeds the project budget and the risk needs to be raised to NREN stakeholder level to decide the appropriate quantitative analysis approach.

In the case of green risks, there is no need to allocate the full budget and other resources for each of the individual risks in this category. A good approach is to allocate a contingency sum in the original budget to cover all the green risks, calculating the individual cost of the risk scaled by the risk's probability.

Bearing this approach in mind, the original budget for the cloud strategy implementation needs to be extended to include the results of the quantitative risk analysis based on the response costs of red risks and the contingency costs of green risks.

In our examples, both risks are in the red category and response actions are mandatory (to reduce and to avoid the risks), and therefore the full amount of response budget is needed to implement the response plans.

7.3.5 Risk monitoring and control

While the previous steps in risk management deal with the analysis and planning that need to be included in the NREN cloud strategy, risk monitoring covers those actions required to keep the risks manageable, and this is an ongoing process during the whole project implementation lifetime. If the appropriate risk planning is carried out, half of the job is already done in the case that a risk does occur – the risk is predicted, response actions are defined, budget is allocated, the stress and negative consequences are minimized. It is much better not to wait for a risk to occur, but rather permanently monitor the identified risks and indicators, review the risk probability and impact, update the risks status, improve the response actions and identify new risks. With proper risk monitoring and control mechanisms, the right actions can be implemented in advance to avoid the risk or trigger the response actions at the right time. It is also necessary to communicate periodically a report of the risk monitoring activity to all stakeholders and staff, throughout the project lifetime.

8 Supporting Actions

8.1 Organizational changes

The IT landscape is changing at an ever increasing pace, offering organisations and individuals new services and opportunities but also bringing with it new challenges compared to traditional IT models. NREN activities in this arena may include the direct provision of Cloud Services or Brokerage of Cloud Services from commercial service providers or other NRENs. Many aspects of Cloud Services – particularly in the area of SaaS are well established and mature e.g. Public and Consumer cloud services such as Gmail, Office365, AWS while many other services and solutions are still in their infancy e.g. Private/Community cloud, Cloud Service Brokerage (CSB) with many open issues in terms of interoperability, security and standards.

Many NREN organisations have evolved around the central theme of the network as the core service. The importance of the network has not diminished and in the era of Cloud Services is even more critical. Cloud Services however bring new challenges to NRENs both as a consumer and service provider and the organisation, skillsets and even the business model may need to evolve as the consumption of cloud services by end user individuals, institutions and vendors becomes more and more pervasive.

Cloud Services cover a broad range of possibilities and each NREN must define its own Cloud Services Strategy. To be able to deliver on its Cloud Services Strategy, NRENs will need to develop the appropriate level of internal competencies to cover the full lifecycle of potential new services from Concept to Production. This may include some or all of the following capabilities:

- Understanding of the potential of Cloud Services and how to apply it to develop the local NREN strategy and communicate it to client institutions
- Cloud Service Brokerage skills – to engage and manage service providers as well as evaluating the broad range of potential products and services from infrastructure to applications.
- Security and Technical skills in Cloud Technologies appropriate to the relevant Cloud Services e.g. Platform Specific skills to Test, Implement or Operate cloud services, Storage, Billing etc.
- Service Management Skills to manage external service providers
- Governance, Commercial, Legal and Contractual skills

NRENs may have some or all of these competencies in-house but the organisation structure may need to change to reflect the NREN strategy and impact of Cloud Services on skillsets and resources.

8.2 Cloud Financial Model

The financial model for cloud services is an area in which NRENs may need to take new and innovative approaches to the business model depending on the service. NRENs will generally need to make a business case for each cloud service to validate the viability of the service and the corresponding financial model.

Traditional IT and network services tend to have long term commitments by clients and predictable costs and charges. In the cloud world however services are in many cases provided on a utility basis i.e. “pay-as-you-go” or “on demand” as users consume resources. This unpredictable nature of cloud services makes it difficult to devise a financial model for a cloud service – especially one which is new, for which the demand is not clear,

and in the absence of clear commitments from clients may even represent a “build it and they will come” approach. An example of this model is the experience of the public cloud services e.g. AWS where users can pay for VMs on an hourly basis. The pricing model for AWS is potentially quite complex with a multitude of service components which influence the final price for end users including time commitment, storage, network traffic, VM size, IP addresses etc. The unpredictable and complex nature of public cloud service pricing may be an opportunity for NRENs to provide a differentiated service by offering a simpler more transparent model.

Where Cloud Services are provided by a brokerage approach, the business model may be much less complex as the Cloud Service Provider is taking responsibility for the complexity and unpredictability. In this case the NREN should be providing some added value to clients e.g. aggregating the demand of clients, better commercial/contractual conditions, provision of federated access, providing hosted capability etc. and NRENs may need to charge for this.

Key elements of the financial model to consider are:

- Funding (e.g. full, partial) availability and constraints
- Pricing model
- Billing or chargeback requirements

8.2.1 Funding Model

A starting point for the financial model is the NREN funding environment, for example:

- Has full funding been provided for the cloud service(s) e.g. by the government or NREN which will cover the full service costs. In this scenario billing may not be a concern but mechanisms to monitor and control usage of cloud services will still be required.
- Has partial funding been provided for the cloud service(s) e.g. by the government or NREN. In this case the shortfall between funding and CAPEX and OPEX costs will likely need to be covered by generating some income from the cloud service(s).
- If no funding is available then the NREN will need to fully cover its costs by charging users of the cloud service(s). In this case ”users” most likely means user organizations (NREN members) rather than individual users.

In the Cloud Service Brokerage approach the service is likely to be self-funding. In this model the NREN is brokering a service from another NREN or a commercial vendor so the funding complexity and risk is much reduced. The NREN may still need to recoup costs incurred in tasks such as project or service management but potentially still offer a service to its clients which is attractive and commercially competitive due to discounts or other benefits such as federation, favourable contractual terms, peering etc.

8.2.2 Pricing Model

As mentioned previously, cloud services bring new challenges to NRENs based on the utility model i.e. consumption based which can be highly variable. NREN clients are used to pricing models of SaaS and IaaS providers where pricing is based on the number of users or accounts, storage used, virtual machine sizes and quantities. Pricing for some services may be on an hourly basis for example a researcher may initiate (using automation) 200 large virtual machines running a Linux operating system, use them for 3 days worth of computation and associated storage and then shut down everything.

The NREN service provider may therefore need to construct a pricing model providing the end user with a price which considers the resources consumed including CPU, Storage, Networking and software licenses as well as general service costs e.g. support, power, hosting charges, infrastructure etc. Commercial pricing models e.g. AWS, are complex and unpredictable. One variable, particularly for IaaS services, is the network traffic used by the cloud which can be difficult or impossible to predict. NRENs who provide cloud services e.g. IaaS Storage or Compute, have the opportunity for differentiation by providing certainty for clients through fixed or zero network charges as this is existing core NREN infrastructure.

NREN clients can be expected to use public services such as Microsoft Azure or Amazon AWS as pricing references. This is a potential risk as public cloud pricing can seem very attractive e.g. AWS offers, at time of writing, $0.15 per hour for a virtual machine. For real world deployments however NREN clients must estimate the individual costs of all their requirements, including for example support, IP addresses, storage, backup storage, archival storage, network traffic, database I/O, DNS queries etc. as well as resilience or performance requirements beyond the basic level. NREN clients therefore may be using unrealistic figures based on incomplete estimates of public provider costs. Most service providers provide online calculators to show the pricing model (e.g. Microsoft Azure[4]).

Despite NRENs not being required to generate a profit, they are unlikely to be able to compete with public providers unless funding subsidises costs (as do many public providers). Based on feedback sources such as Gartner, NREN clients can however be expected to be prepared to pay a premium for NREN services based on key differentiators such as:

- Security – data location/privacy, security audits/compliance, national regulations etc.
- Support – while basic public cloud provider costs are very low, standard support is typically self-service with additional options costing more. NRENs on the other hand typically provide a high quality service from a known organisation.
- Federation – support for eduGain or local equivalent services
- Performance – high performance service delivery across GÉANT network
- Availability
- Network - potential for no or fixed network charges
- Non-profit/community motivation focused on the Education & Research sector
- Currency – pricing in local currency
- Cost Transparency – potential for simpler pricing model (compared to public cloud vendors) without network transit charges
- Invoicing – whereas some public cloud providers expect payment by credit card

Pricing of cloud services is therefore an area for major consideration and potentially quite complex.

8.2.3 Billing Model

Billing requirements and approach will be dictated by the pricing model and can be complex e.g. the requirements to provide a service priced per hour or per Gigabyte of storage used will potentially create a significant task to quantify usage to provide the input to billing.

Billing systems used by service providers are in general a cause of considerable complexity requiring expertise and resources. The effort in meeting billing requirements can be significant and the negative implications

[4] http://azure.microsoft.com/en-us/pricing/calculator/?scenario=full

associated with billing mistakes can be considerable. **NRENs should carefully evaluate the complexity and robustness of billing functionality required to deliver services either directly or brokered with third parties.**

In addition to the complexity of billing driven by the pricing model, business or client requirements may also drive additional billing requirements such as:

- Reporting – to provide supporting information on bills e.g. usage statistics
- Fixed period discounts e.g. for monthly or annual commitments to service usage
- Prepayment for services to fit with client budgeting requirements and planning
- Penalties/Service credits for not meeting service delivery targets
- Integration with external billing or service reporting systems
- Credit card payments in case of billing individual users

As discussed previously, NRENs also have the opportunity to adopt simpler pricing models and reduce complexity. An example of this is the HEAnet Edustorage service providing, at time of writing, storage at €275 per TB per annum or pro rata (Appendix A.1).

Many NRENs may have a requirement to implement a Chargeback functionality whereby their member institutions will require bills to be generated according to their organisation and/or billing structures e.g. departments, cost centres or even individuals. In some cases they may wish the NREN to send bills directly to that department, cost centre or even individual. This approach should be considered carefully (and in general avoided) by the NREN due to the contractual arrangements and the practical complexity/risk of following up on payment. The NREN client also may wish to receive bills in specific formats that can be incorporated into their own internal billing mechanisms.

8.3 Service Branding

The cloud services world is a crowded arena with many service providers competing to get the attention and business of the NREN client base. While NREN clients are in general loyal and an existing customer base, there is no guarantee that they will choose or even understand the cloud services being offered by the NREN. The NREN will need to compete with strong messages from commercial providers to ensure its clients understand its strategy in relation to cloud services and what it can offer its clients and the key benefits. To ensure its messages reach the right audience the NREN needs to consider:

- The Service branding and key messages
- A Communication strategy to deliver the key messages

The above topics are no different to those facing the commercial providers and the approach is similar. The branding of a service helps NREN clients understand its positioning and the unique value that the service brings e.g. low cost, high performance, ease of use, security etc.

Communicating the service brand and key messages is a significant ongoing task and will likely require a combination of approaches including:

- NREN conferences e.g. presentations, demos, workshops
- Dedicated website
- Newsletters
- Email distribution
- Individual client meetings

- Whitepapers and case studies

The above mentioned communication methods are out of the scope for this document, but it is worth emphasizing that engaging clients early in the service development process is important to ensure the service meets their requirements as fully as possible. The early engagement, for example in feasibility studies, proofs of concept, will help raise awareness and make cloud adoption easier. The more clients understand and where realistic have an input into service definition, the more they are likely to use the finished product. This ultimately leads to greater take up of the cloud service(s) which will usually generate economies of scale which will help make the business case as realistic as possible.

8.4 Service Assurance

The NREN client base will potentially have a broad range of use-cases within their own user community, from IT department requirements to financial, research, teaching etc. The demands of the many and varied use-cases are likely to vary from low end, commodity and best effort requirements, to high end computing, mass storage and business critical requirements. As clients seek to leverage the benefits of cloud more and more and the technology matures, they will increasingly add more critical and demanding use-cases to supplement or even replace their own IT landscape. The more the client depends on the service(s) offered by the NREN the more it is likely to seek to ensure that the cloud service can deliver on the requirements of the business, which will typically mean uptime, performance, value for money, flexibility, scalability etc.

NRENs therefore need to consider Service Assurance as part of their service offering to their clients which may include:

- A SLA with service targets on KPIs e.g. service availability hours, availability uptime, latency, helpdesk response, billing accuracy
- A service mechanism to deal with service requests e.g. ITIL helpdesk
- Service monitoring and reporting tools for clients
- Service penalties/credits for not meeting service targets
- Service Management reporting
- Service Management resources e.g. for helpdesk, service meetings with clients

In many cases NRENs will have an established service delivery and management capability. Cloud service(s) while new and perhaps different to more traditional services should be able to fit in with an established service environment with limited impact. Cloud services in general will work or can integrate with established tools e.g. Nagios, Cacti, Zenoss, Syslog etc. but may require some integration or development effort.

9 Summary

Cloud computing is profoundly changing the traditional way IT services are acquired and consumed: this trend is foreseen to continue for the near future, and is expected to be even more disrupting than we can possibly imagine today. The innovative and pervasive ways in which cloud computing is enabling users to acquire, link and aggregate services and information are changing the way users work, interact and produce new knowledge.

GÉANT and the NRENs were created out of a community to serve the community's needs: therefore, it seems natural for a NREN to define its attitude to cloud computing and take an active role in helping the user community to uptake and use cloud services for research and education.

The cloud is happening "now", so this is the right time to make the transition. As was discussed in this document, however, NRENs should be aware that "going to cloud" involves a mindset change, shifting the focus from "IT product" to "IT service", which does not only nor mainly involve technical issues and impacts all business processes of the NREN. At the same time, "going to cloud" should be regarded as a highly dynamic process.

In this document we have tried to provide the elements to help each NREN draw a recursive path running through the following steps:

- Observation: Strategy Analysis Phase
- Planning: Strategy Formation Phase
- Doing: Strategy Implementation and Supporting Actions
- Checking: analysis of results as measured in the "Doing" step, with respect to goals set in the "Planning" step
- Adjusting: the feedback loop needed to provide continuous improvement

Finally, in the last part of this chapter and in the Appendix we have collected a set of recommendations and a varied set of "Inspiring Stories", representing the essence of the experiences of some NRENs in the field of clouds. Although we are aware that the landscapes in which NRENs operate differ tremendously, we are confident that studying other NRENs' experiences may shed some light to some specific spots which may be relevant to your NREN, as well as provide concrete examples as to how the approach to strategy formation described in this document translates in the real life.

The cloud is here, and it is here to stay, at least in the medium term. We are confident you will find this document valuable to make your journey to the cloud successful and safe, for your organization and your users.

9.1 Recommendations:

1. NRENs should have clean and continuously updated assessment about their community opportunities and threats and subsequently prioritise how they can help their community.
2. NRENs should educate their community about the cloud, available cloud services, how to apply it to their work, how others have been successful, and how to be effective.

3. As highlighted in several “Inspiring Stories” presented in Inspiring Case Studies, users’ involvement at different stages of the strategy analysis and strategy formation processes is an essential element in ensuring that, eventually, the cloud offering effectively addresses users’ needs and the NREN cloud services can be potentially relevant to them: however, it is not the only ingredient, and specific supporting actions need to be deployed to enable users to adopt and consume such services.
4. NRENs need to define their own security and legal framework requirements identifying their technical, practical and legal constraints. Failure to having clear definition for them can present serious challenges as most cloud services providers rarely deviate from the signed contract.
5. NRENS should continuously enhance their network infrastructure, meeting the reliability requirement of the services offered.
6. NRENs should use the business model to undertake an initial threat and risk assessment. The risk management guidelines for cloud services (see 7.3) can be used for this purpose.
7. NRENs need to work as a Cloud Explorer, doing assessment of current applications which meet the education sector needs and promote their uptake.
8. NRENs need to work as a Cloud Enhancer by conducting POCs and pilots to mitigate the risk of adopting new services.
9. There is no single cloud deployment model that is ideal for all NRENs’ needs. Therefore, it is recommended to consider utilising a range of different public cloud services while simultaneously preparing to build community cloud infrastructures (multi-layered cloud implementation approach). Data should be placed in the right type of cloud (public or community). NRENs may start with brokerage with the service providers for the services that can be migrated easily and prioritise those migrations that have the highest value to the business (e.g. heavily used applications, standard applications and services).
10. Irrespective of having its own community could or not, it is recommended that NREN plays as a demand aggregator in the national base and try to get the best deal, by acting as a broker, for its community. This can include Contract templates; checklist of “contract deal-breakers”, procurement tips, decision tree/checklist of “Questions to Ask,” and list of preferred vendors for specific solutions so no NREN user feels like she is starting from scratch.
11. NRENs cannot and should not compete with cloud service providers in the market. However, most institutions have concerns about data security and regulatory/compliance concerns and are not willing to migrate all their data to the public cloud. A private cloud deployment model - whether owned as on-premise infrastructure or sourced as a managed service - is often the preferred model for handling sensitive data. However, if a private cloud is built in-house then it will require excess standby capacity and capital costs. By having accurate assessment about its community need, NREN can provide a community cloud for the data that are of strategic importance or subject to regulatory conditions (i.e., personal data, sensitive data, or strategic data). The trust established between NREN and its community can serve well for this purpose.
12. NRENs community cloud should focus on systems and applications where high levels of customisation and/or strict requirements apply. The process can start with implementation on a small scale with limited groups of users to test new services.

13. Related to point above, NREN should take advantage of its community's capabilities and expertise in creating/tailoring services that meet its community needs better than the ones available in the market, if any.
14. Once the cloud strategy has been setup it is very important to communicate it both internally within the NREN and externally to (potential) users. Experience tells that not all NRENs decided to produce a formal Cloud Strategy Document, in any case the key messages which should be conveyed are: "why" is the NREN getting involved with clouds, "who" is the community addressed by the offer, "what" are the available services, "how" the services will be provided (technical and legal aspects, SLA, resulting benefits,…).
15. NRENs should take full advantage of X-a-a-Services offered by other NRENs. GN4 activities can be a good driver for disseminating the information and facilitating the use/duplication of services offered by other NRENs.
16. It is recommended that while dealing with the market players, Dante places some sort of high-level negotiations and provides a framework for the cloud services they offer. NREN may find beneficial to have access to this framework and take advantage of negotiated deal for its community.
17. As the market is very competitive and evolving rapidly, it is highly recommended that NRENs be fully updated and take advantage of cutting-edge technologies for interworking between clouds. Not only does this prevent the lock-in problem, but also it is in line with the multi-layered cloud delivery model approach discussed in Section 6.4.5, facilitating the possibility of having interconnected pan European clouds of NRENs through GÉANT backbone.

Appendix A Inspiring Case Studies

A.1 EduStorage and Cloud Compute at HEAnet

HEAnet has been offering Storage as a Service (STaaS) - EduStorage - since mid 2012. EduStorage is a block storage service and provides storage on demand for Irish clients who are using it to provide primary and backup storage. The infrastructure consists of two resilient IBM SANs providing a total of 500 TB capacity spread over two datacentres. Connectivity to servers is provided by iSCSI and federated access is provided to administrators (limited to IT staff) for self-provisioning to easily add, delete, or modify volumes via a self-service portal. The service has been widely adapted by HEAnet clients and the performance, capacity, ease of access and attractive pricing (€275 per TB per annum) make it a popular service. EduStorage is attractive also as it is available and charged on demand i.e. as a Utility service and removes the need for clients to have SAN storage expertise. Performance is almost as good as a SAN based locally on the campus due to the low latency (< 10ms) across the backbone network.

The EduStorage service originated out of discussions with clients identifying the need for a flexible Storage as a Service solution from HEAnet. HEAnet implemented a framework procurement process which was then used to select the supplier. The framework has subsequently been used by clients to simplify and speed up procurement of their own storage infrastructure. Following a Proof of Concept phase and a soft launch, the service was released in mid 2012. Most clients have adopted a cautious approach starting with a trial and most have subsequently moved on to production usage. Issues experienced have been mostly around providing the correct access to the campus resources for iSCSI connectivity which typically required reconfiguration of client devices and firewalls rules in particular.

The service has proved to be very robust and is backed by a small support team in the Managed Service (MNS) group to ensure the SLA is achieved. The service was promoted extensively with clients in direct meetings, conferences, newsletters, workshops as well as a dedicated website https://www.edustorage.ie/. Further enhancements are in consideration subject to client discussion including a file-sync type capability and integration with HEAnet's future Cloud Compute service.

The main lessons learned have been that although pursuing a framework agreement approach has provided benefits to clients, it added complexity and time to the overall project due to the effort required in fulfilling the legal requirements. The customisation to implement federation was seen as a major risk but in reality went very smoothly. Much of the difficulty and support effort has resulted from setting up the initial client connectivity to the SAN which typically required investigation and reconfiguration of network devices. Once setup, however, the experience has been that the service is easy to use - it is simply another disk as far as the IT staffs are concerned.

As a follow on to Edustorage, HEAnet has considered another Infrastructure as a Service – Cloud Compute, i.e. providing Virtual machines in the cloud. The initiative for Cloud Compute was driven by customer requests i.e. the demand for VMs. In the case of HEAnet, it was already using a Virtualised environment based on VMware however this was not suitable for providing VMs to clients as a) this is not compliant with the VMware license b) it was not a multitenant solution.

Some of the key decision points for HEAnet in relation to its strategy and services are highlighted in the following Q&A:

Q : What is the strategic approach to cloud for HEAnet?

HEAnet see cloud services as a major trend affecting almost all levels of its client base from: students to lecturers, researchers and IT staff. HEAnet clients are currently leveraging cloud services and this trend will continue to increase in terms of cloud adoption. The adoption of cloud services brings opportunities and threats to HEAnet and its clients and HEAnet's role is to help clients achieve their business goals by maximising the opportunities of cloud regardless of the type of cloud service or provider i.e. cloud neutral.

Q : What is the model for implementing the HEAnet cloud strategy?

HEAnet believe that there will be no one cloud provider in a position to meet all client requirements and clients will use a variety of cloud providers and models to meet their requirements including public, private and hybrid. This requires a multi-layered approach:

- Brokering of services with public cloud providers and other NRENs. Brokering may include getting standardised Terms and Conditions (T&Cs), optimising discounts or on a technical level for example technical features such as federation or peering to maximise performance.
- Build services where they do not exist or HEAnet has unique benefits compared to commercial providers.

Q : What types of services should HEAnet offer its clients?

HEAnet clients have a wide variety of needs for services which span the full range of SaaS, PaaS and IaaS. The decision on which cloud services HEAnet should deliver directly was based on:

- What is the differentiator with HEAnet for the service in question compared to market offering e.g. price, performance, security, functionality. It was concluded that HEAnet could not and should not compete with the market. The main differentiators (compared to public provider service offerings) were network performance, federation, data location.
- What is realistic in terms of cloud services for HEAnet to deliver directly. It was concluded that in terms of SaaS, PaaS and IaaS potential services, IaaS options i.e. Storage and Computing were the most realistic options. The dedicated skillsets and resources required to deliver PaaS and SaaS options were not viewed as viable. The exception to this was VLE (Virtual learning environments) where HEAnet has a longstanding core expertise in Moodle and plans to offer Moodle as a Service.

Q: How can HEAnet avoid the time and cost to build up dedicated pillars of expertise to build and support a Cloud Compute service?

As HEAnet does not have the available resources to develop, build a Cloud Compute service and provide support on a 24 x 7 basis, it was decided that the most cost effective and least risky solution was to buy an "off the shelf" cloud solution including support from a vendor by conducting an RFT.

Q : How to address technical risk e.g. immature and unproven technology as well as the business risk that there may not be enough client demand for a service and as a result the business case is not viable ?

Start with a Proof of Concept (POC) to provide clients with access to a service prototype on a limited basis i.e. without the scale and all the requirements of a full production service. The POC should be free of charge to HEAnet clients to reduce risk and lower the barrier to entry so that clients can test use-cases and provide feedback on functionality and the requirements for a potential future service. A requirement of participating in the POC is that clients provide feedback on use-cases to the community and provide a forecast (without commitment) of expected demand for a future service.

A.2 Okeanos at GRNET

Okeanos [15] is an Infrastructure as a Service (IaaS) offering virtualized computing resources. It is developed by GRNET, the Greek Research and Technology Network. GRNET plans to offer Okeanos to the whole Greek research and academic community. It is already in place with most of the services available for Okeanos' end users.

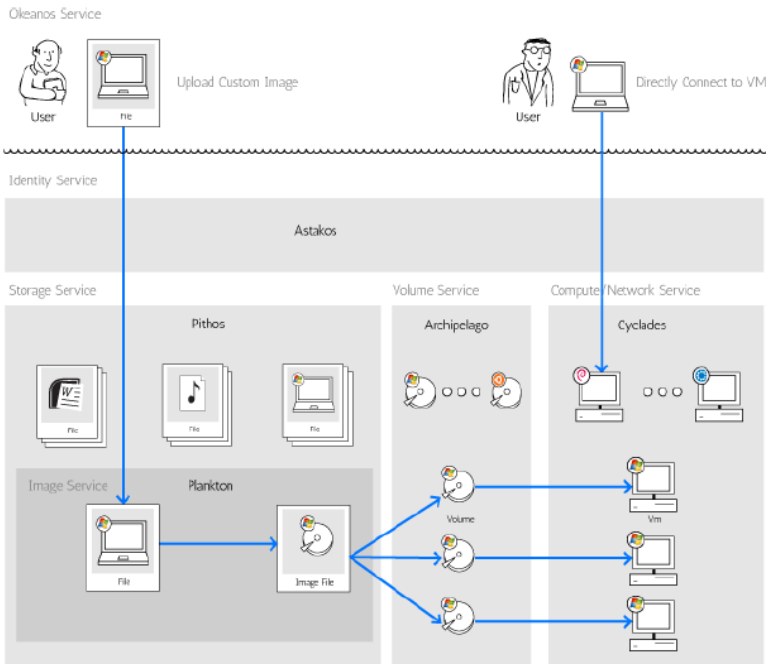


Figure 6: Okeanos Overview

GRNET provides several services to the Greek academic community regarding network, storage and other services [16] which are combined with a number of activities (monitoring, issue handling, helpdesk operations) to deliver the end-user experience. GRNET with Okeanos will provide the Service Level Agreement (SLA) service to its users with a management team that will lead this work in Okeanos.

The **Compute Service** of Okeanos, which is called **Cyclades**, combines a backend for VM cluster management with a custom UI implementation for the frontend. For the backend part, Okeanos is using Google Ganeti, a scalable and proven software infrastructure for managing VMs in production environments. Inside Okeanos, users have access to VMs which are powered by KVM. The VMs are accessible by the end-user over the Web or through a REST API. Users have full control over their VMs (e.g. create, start, shutdown, reboot, destroy). They can also configure the properties of a VM, such as the number of CPUs, RAM, the size of disk, operating system. The REST API for VM management is OpenStack compatible and has been implemented in Python with the Django framework. The Okeanos UI is written in Javascript/jQuery and runs entirely on the client side. Each VM supports dual connectivity IPv4/IPv6 and platform-provided firewalling. Users also can create multiple private, virtual L2 networks in order to construct arbitrary network topologies. The networking functionality is exported all the way from the backend to the API and the UI.

Archipelago is an Okeanos service for handling **storage Volumes** for VMs as a hierarchy of snapshots and clones. Every Volume inside a VM can be thought of as an addressable set of fixed-size blocks. For the actual

storage of blocks Okeanos is using RADOS [17], a distributed object store underlying the Ceph parallel filesystem, in order to keep a reliable, fault-tolerant object storage.

Pithos+ is Okeanos's **file storage service**, an implementation of the OpenStack Object Storage API. Every file is stored as a collection of content-addressable blocks. A client may identify the parts of files which have changed either locally or remotely, and upload or download only the modified parts. Pithos+ comes with a full set of Web-based, command-line and native clients, all making calls to the same API. Both system images and user-provided images are files on Pithos+.

Plankton is the **Image Registry** for Okeanos. Every image on Plankton is a file on a Pithos backend, with special metadata. Plankton implements the OpenStack Glance API and in the current version Plankton and Pithos run on a single, unified backend. Users may synchronize their images with Okeanos using the Pithos' clients and register them in Plankton, with zero data movement.

Some of the key decision points for GRNET in relation to its strategy and services are highlighted in the following Q&A:

Q: What is the strategic approach to cloud for GRNET?
A: GRNET plans to build a real world community IaaS to the end user. Okeanos will be the first IaaS provider for the research and academic community in Greece. All researchers, professors and students will use the facilities of Okeanos for their experiments and also for educational reasons.

Q: What is the Okeanos business model?
A: GRNET provides the Okeanos cloud services to the Greek research and academic community free of charge. More specifically, there are two target groups that are using Okeanos facilities:

- IT departments of connected institutions
- University students, researchers in academia

GRNET will adapt policy models for all target groups delivering the services with the appropriate SLA services for a better quality for all users.

Q: What types of services GRNET offers to its clients?
A: GRNET offers a wide range of IaaS services: Network Service, Compute Service and Storage Service. Through these services Okeanos provides resizable compute capacity and storage in the cloud, making cloud computing easier for users and developers. GRNET plans to provide all these services to the end users and to operate these services 24 hours a day, 7 days/week.

Q: How to address technical risk e.g. immature and unproven technology as well as the business risk that there may not be enough client demand for a service and as a result the business case is not viable?
A: GRNET made several trials with the users before the cloud services were established to the Greek community and all problems that arose in the trials were solved before the services were made available to the end users. With that given, Okeanos could be in a real production environment since all services have been tested before the production time.

A.3 Vscene at Jisc

Based on the conducted study, a shared services approach has enabled the HE community in the UK to save over £66 million in 2012 by providing a centralised videoconferencing service. The service has evolved over the last 15 years to become a feature rich service fronted by an automated videoconference management system. A reinvented version of the Jisc videoconference service, Vscene, is ready to be offered as a service to other

NRENs, helping them to connect their user communities together while minimizing the CAPEX and/or OPEX of providing the service.

Vscene attempts to hide or remove most of the confusion found in scheduling conferences between multiple VC system types. With Vscene, there is no need to know what type of VC system your collaborators have, or mess about with dialing long numbers. This is NREN grown videoconferencing without any fuss. Users can schedule or launch a conference exploiting any of the service features, including recording and streaming, and add participants and guests in any combination of interoperable videoconference standards. Intended to serve beyond the Jisc community, Vscene offers Multipoint Control Unit (MCU) scheduling as a cloud service, and NRENs can use the service as a user interface to their MCU resources, offering their users easier conference management and more control in the connected world. This cloud scheduling approach enables NRENs to still use their own MCUs for their users, but also potentially allows access to a wider international pool of MCU and other resources at times of high demand.

HEAnet, being a major consulted stakeholder in the development, is the first NREN to take the service up. HEAnet uses the service as a user interface to their MCU resources and to offer their users easier conference management. Vscene cloud scheduling approach enables HEAnet's own MCUs to be prioritized for their users, but also allows access to a wider pool of MCU resources across the UK at times of high demand.

Currently on Vscene there are over 8,151 registered videoconference systems and over 9,866 users across 1,112 organizations (in the UK and Ireland). The service manages approximately 50,000 videoconferences per year via its centralized infrastructure for its internal, as well as external customers.

Vscene can currently interoperate between ISDN, IP and a Desktop client. IP endpoints can be registered using IP address, e.164 (Global Dialing Scheme) or SIP URI. Jisc is also working with NRENum.net as a longer-term global scheme. The service has been historically provided by using Cisco infrastructure, and in addition to this now Vidyo infrastructure is used to provide a significant feature set within the service. The Vscene development team have worked hard to master the API set provided by each manufacturer and are also open to work with additional video hardware and APIs to make Vscene more flexible and useful to a wider party of NRENs. Along with other Vidyo technologies, Vscene utilises the VidyoWeb browser plugin to provide a free and scalable desktop client for the entire Jisc community. The browser plugin has proved very popular as it does not require administrative access to download and uses a Scalable Video Codec (SVC) which can provide excellent quality video in environments where bandwidth may previously have restricted the use of VC.

Some of the key decision points for Jisc in relation to its strategy and services are highlighted in the following Q&A:

Q: What is the strategic approach to videoconferencing for Jisc?
A: Jisc has been providing the education and research sectors an interoperable video conferencing service for 15 years. A new version of service launched in 2014, made Jisc the first NREN to provide a cloud based service to the GÉANT community. The main elements of the Jisc strategy is to position Vscene as an interoperability hub by offering bridging to as many third party technologies as possible, to provide a world class feature set and user interface and to make significant cost savings for the education sector by promoting the growth of large scale use of videoconferencing across Janet.

Q: What is the Vscene business model?
A. The service was available free at the point of use to all members of its community, and continues to be free in its new version. However, an annual based fee is applicable to external organisations/NRENs. As central funding for the service is not expected to be maintained in the longer term, Vscene will be available at a per organization charge to Jisc connected community sites.

Q: What types of services Vscene offers to its clients?

A: Vscene offers following features:

- Standards based Videoconferencing pre-scheduled or on demand
- Live conference management tools
- Desktop client (browser based)
- Recording
- Streaming
- Personal virtual Meeting Rooms
- Operator support for all conferences

NREN Services

- Cloud-based MCU
- MCU management interface
- MCU integration
- User migration
- Interface language translation
- Branding options
- 99% Videoconferencing service and booking service availability
- 99.5% Gatekeeper hierarchy and gatekeeper service availability

Q: How to address technical risk e.g. immature and unproven technology as well as the business risk that there may not be enough client demand for a service and as a result the business case is not viable?

A: Technical risks are mitigated by the use of proven service class infrastructure and long tested technology. Risks in the interface design and in interfacing with the infrastructure are dealt with by identifying API support expertise and using infrastructure that already has a strong API set.

A.4 u:cloud at ACONET

The University of Vienna, of which ACONET is part, is offering OwnCloud to its community. We have the Enterprise edition, which allows us to have a branded version which we call **u:cloud** (http://zid.univie.ac.at/ucloud/).

We started with version 6 in April of 2014. We tested this version for two or three months with about ten people from the computer centre; subsequently we invited other colleagues from the university that were interested in cloud services, and performed further tests for the remainder of 2014. During this time, we also updated the service to version 7. Overall, about 50 people throughout the university were involved in the testing phase.

The official service started in January 2015, and we currently have about 150 users.

Q : What is the strategic approach to cloud for ACONET and how did you implement it?

We decided to offer cloud services to our community in anticipation of growing needs; we did not receive any direct requests for this, but we knew that some research groups needed it because of their involvement in international projects.

We have also been involved with the TERENA cloud activities, specifically regarding the OwnCloud offer. During 2013 we tested a number of cloud systems and ultimately settled on OwnCloud, both for technical reasons and because it is a popular choice among NRENs and other universities in Austria.

Very early on we decided to opt for the Enterprise edition of OwnCloud, for several reasons: (a) we believe the service provided under this version is a good value-for-money, with competitively-priced licenses, (b) we wanted a branded version of the service, and (c) we wanted our researchers to be able to get the mobile client for free.

Q: What is the ACONET business model?
The service is free for our community, and the University of Vienna covers all related costs, which are largely based on the cost of the storage system. We actually have a cheaper version of the storage service, and not the Enterprise version.

Q: What impact has this had on your organization?
Currently we provide the service on a best effort basis. This is very hard for us, and we are very aware that we need additional staff. Specifically, we need one person who is dedicated full time to the service. We have made a request to the University Rectorate for this new position, but we have not obtained it (yet).

Q: How do you address issues of scale?
As of January 2015, we are offering this service to our faculty and staff, which numbers about 10000 people. We believe we have enough storage for this community. In terms of server performance we are less sure: when this service becomes really popular we will have to change the current setup for object storage; in order to do this, however, we would need to hire this new person.

Q: Can you share any lessons learned?
We are still learning every day. One thing we have seen is that the original setup with native OwnCloud object storage was not possible for us; this is a problem we already knew about, and the solution – redoing the setup – is not something we can solve without the new hire.

Q: What are your plans for the future?
We want to show that this is a really good service, to bring our case to the Rectorate, thus reinforcing our request for the new hire, and eventually extend the service to our student population, and hopefully other institutions in Austria. There are other universities in Austria that use OwnCloud. if we can show the universities how good and useful the service is, they will hopefully support us in expanding it.

Q: How are you working with the GÉANT SA7 cloud activity and how do you benefit from this?
We are in contact with them. We went to the workshop last year, and we communicate regularly with various SA7 people; we see the activity as a solid knowledge base, and a place where we can exchange experiences.

A.5 Refining Cloud strategy at SURFnet

SURFnet has recently changed its cloud strategy, in the sense that now we offer our members a fuller spectrum of services.

A few years ago, inspired by a study trip to which we invited managers from member institutions to the US, we decided to adopt – and recommend to our stakeholders – a Cloud First strategy, whereby if an institution needs a new service they would look at what is already available from the public (i.e. commercial) cloud providers. SURFnet would support them in this strategy by having a vendor management team functioning as broker towards a relatively broad set of vendors, working to ensure features such as data protection and favourable pricing.

What we have seen however, is that this particular strategy hasn't really taken off. Institutions are hesitant to move to the public cloud, in part because they don't feel that it's safe enough: they want data stored in the Netherlands, better access control and better guarantees in general.

We have been asked specifically to provide a personal cloud storage solution as an institutional alternative to the widely used DropBox, which our members would like to discourage among their communities, for security reasons. Thus we created SURFdrive, based on OwnCloud, to satisfy this request. This was our first experience in creating a service directly in response to a request (technology pull).

In connection with this we have established a new, systematic procedure for creating and implementing new services for our community within the SURF Cloud programme.

Q : What is the model for implementing the new SURFnet cloud strategy?
Our new procedure includes a full spectrum of cloud delivery models, maintaining the public cloud option (via SURFmarket) but in addition offering community cloud services such as SURFdrive, or a "mix & match" approach that combines parts of both. For each delivery model we (try to) implement SURFconext (our identity federation) and make it compliant with specific legal norms for higher education that cover issues like privacy and data ownership.

Our procedure lays out the provision of a new service in a set of logical steps and checkpoints, which include the formation of a small group of "early adopters" of the new service, a requirements analysis, the elaboration and selection of a delivery model which will determine whether a new service needs to be developed, and the eventual addition of this new service to the existing SURF Cloud services.

If as a result of this process it is determined that a new service needs to be developed, the institution(s) can request a custom development project, which will be carried out in collaboration with SURF.

Q: What is the SURFnet business model?
It depends on the delivery model: for the public cloud component, the institution will pay for the service according to the favourable conditions we negotiated. For a community or 'mix & match' project, there is a mix of cost-sharing in terms of dedicated manpower from SURFnet and the institutions involved, plus the latter will pay for an external project leader, who is brought in as an objective party, and for the personnel who undertakes the development work. Once the service reaches production status, the costs of the service will be borne by the institutions that use the service.

Q: What impact has this had on your organization?
SURF Cloud is a new programme within SURF. One of the product managers from SURFnet, who was previously responsible for a range of services is now focused specifically on cloud services. In terms of representation, the cloud services area is common to all the SURF organizations: SURFnet, SURFsara and SURFmarket. Each of these SURF organizations brings in resources and has committed to making the SURF Cloud programme a joint effort.

Q: How to address technical risk e.g. immature and unproven technology as well as the business risk that there may not be enough client demand for a service and as a result the business case is not viable?
This is encoded in the new procedure, which includes a feasibility analysis and might include a proof-of-concept or pilot phase. Of course, the new service will be tested (by us and/or one or more institutions) before it reaches production status. It is also possible, if something is not working out as hoped/planned, that the project can be modified "on the fly" to optimize results.

Q: How do you address issues of scale?

In the case of SURFdrive, we use the hardware at the SURFsara datacentre. Usage is monitored very closely, and we have noticed that growth tends to be moderate and steady; thus it is not difficult to adjust the hardware in accordance with projected needs.

Q: What are your plans for the future?
We are still in the process of adopting this new procedure, so our plans for the future are to more fully embrace this way of doing things. Of course, we are looking forward to working together closely with the member institutions of SURF to make the most of the many benefits cloud services have to offer.

Q: How are you working with the GÉANT SA7 cloud activity and how do you benefit from this?
One thing that was useful was the possibility to jointly purchase the OwnCloud licenses with GÉANT/TERENA and other NRENs; and of course it really helps to learn from all the other NRENs and share our experiences.

A.6 Cloud services in NORDUnet

NORDUnet is the operator of the common Nordic research and education network, connects the networks of the NRENs in the five Nordic countries; UNINETT (Norway), DeIC (Denmark), SUNET (Sweden), Funet (Finland) and RHnett (Iceland), represents the five NRENs in the GÉANT Association and hosts common efforts and collaboration between the five NRENs.

Nordic Level

On a Nordic level, NORDUnet has initiated common procurements for:

- Box. This service has been taken up by Funet, SUNET and UNINETT
- Three services from IPnett (www.ipnett.com); infrastructure, storage and backup. These are in a pilot phase at the moment. NORDUnet and Sunet will proceed with these services, UNINETT is considering joining (and is involved in the pilot phase). DeIC has not yet decided.

In addition to these common procurements, several Nordic NRENs offer or are planning cloud services on a national level:

Norway – UNINETT

UNINETT is coordinating a national effort in Norway in collaboration with the four major universities. The UH-sky (HE Cloud) program aims to expand knowledge and awareness, develop a common strategic approach, as well as deliver concrete services.

At the moment, several services are in the pipeline:

- IaaS – a national service based on the infrastructure of UNINETT and the four universities. Planned to be operational by the end of 2015.
- Unified Communications – a common implementation of the Skype for Business service.
- Feide Connect – an integration service intended to provide additional data to the Feide AAI. Will be operational by the end of 2015.
- UHAD (Higher Education Active Directory) – intended to establish a common service for the Microsoft Active Directory.
- The future storage and HPC services of UNINETT Sigma2 will most likely have a cloud based delivery model.

Denmark – DeIC

The Danish Strategy for Research Data Management has just been adopted by the DeIC board, the research libraries and the universities. Included in the national strategy is five pilot projects aimed at establishing research data management infrastructures for the five scientific areas. It remains to be seen if these services will be cloud services.

There are two concrete cloud services in the pipeline:

- OwnCloud - DeIC has a pilot project based on OwnCloud – called http://data.deic.dk. With federated WAYF user verification.
- Box service - The DeIC board has allocated 1m DKK for 2015 to identify and put into service an "academic drop box", process just started.

Q: What is the strategic approach to cloud for NORDUnet and its partners?
Through the program UH-sky, UNINETT and the Norwegian Universities want to adopt cloud services in a unified manner, to maximize the advantages and reduce the negative effects. The plan is to make this the base for a new service delivery model that in the future might encompass all ICT services in the HE sector.

There are some strategy-oriented descriptions of the UH-sky program, and these may be shared in the community. However, all are currently only in Norwegian. In relation to the participation in the SA7 task, we are looking into translating parts of this.

Research and higher education already uses cloud services, and this use will most likely increase in the future due to the advantages in economy, flexibility, scalability and ease of use. Thus, it's very important to offer cloud services; first in the areas where we already offer services, but we should also look into possible business models in other areas.

Target audience

The target audiences for UNINETTs cloud services are:

- Infrastructure, storage, backup, identity; Primarily IT departments, but in the long run also research organisations and in some cases researchers.
- Unified communications, personal storage, etc.: initially IT departments, but we need to find a model where we can reach students and academic staff and get them to use the services.

Unique selling propositions

- Trusted partner
- Data storage
- AAI integration

Q : What is the model for implementing the NORDUnet cloud strategy?
Services developed completely in-house (within the sector):

- IaaS developed by UNINETT and four universities - Norway
- Feide Connect - Norway

Services developed using Microsoft products:

- UHAD (Microsoft Active Directory) - Norway
- Unified communications (Microsoft Skype for business) - Norway

Brokering services offered by external cloud providers:

- Box – Norway, Sweden, Finland

- Infrastructure, storage and backup services from IPnett – Sweden, Norway

Q: What is the NORDUnet business model?

On the Nordic level initial costs including market research, information gathering, etc., are absorbed by NORDUnet. Costs directly related to each service are fully covered by the NRENs.

In Norway, the same model applies in principle, but in a project phase, some service related costs are absorbed by the project hosted by UNINETT.

Q: What impact has this had on your organization?

For Norway:

- One person employed specifically to head cloud activity. In-house funded project uses approx. 3,5 MY in 2015
- Need to find a business model that is viable for all parties; someone has to pay for the resources we put into a cloud service.

Q: How to address technical risk e.g. immature and unproven technology as well as the business risk that there may not be enough client demand for a service and as a result the business case is not viable?

For Norway: no different than for other services; tender, proof of concept, pilots/trial, etc.

Q: Can you share any lessons learned?

Norway:

Box:

Financial risk: Important to decide before agreement is concluded who bears the risk; the vendor, the NREN or the institutions. Normally a cloud vendor bears all the risk – for a standard service. With adaptation to the needs and requirements of NRENs/HE institutions, there's an extra cost that needs to be addressed. The agreement with box is not optimal for us – we have to guarantee a certain usage, but have no simple means to increase usage. In hindsight this responsibility and risk should have been placed at the institutions – who control the users.

User incentives: With regards to the above – we need to find ways to encourage users to choose the NREN/institution implemented cloud service over commercial alternatives. Why should a student choose our Box service instead of Dropbox, for instance. These incentives can be formal/legal (not allowed to use anything else), financial (unlimited free space/use), functional (security, sharing with groups within the community, federated access, etc.).

A.7 Cloud services at SWITCH

SWITCH has built a scalable cloud infrastructure on top of which we offer IaaS and SaaS services. The service SWITCHdrive is based on ownCloud Enterprise and has been put into production in April 2014. The community received the new service very well. Currently, more than 80 % of higher education members in Switzerland have the possibility to get access to SWITCHdrive. The number of users is growing steadily. The IaaS service called SWITCHengines offers self-service Virtual Machines and storage. Until mid of 2015 it is run as a pilot with test users with the aim to open it to the whole community as a production service beginning the second half of 2015.

The cloud infrastructure is built with open source software as the main building blocks (OpenStack, Ceph). For the hardware SWITCH uses cost-effective commercial off-the-shelf components from the white-box market.

Q : What is the strategic approach to cloud for SWITCH?
SWITCH acts as a provider for cloud services as well as a broker with its role in the procurement for the community. The procurement of commercial cloud services is led by the priorities of the community. From central ICT services in the universities we currently do not see a broad need for commercial cloud services.

The main customer segments addressed are:

- Research organisations
- Academics (teachers as well as researchers)
- Students

SWITCH reaches out to these user groups with the central ICT services at institutions as our partners. The cloud services of SWITCH are seen as a complementary offering to the offering of the IT departments in the universities.

Positioning: SWITCH started 27 years ago as the provider for the academic network that emerged to the connection with the public Internet. As such it has earned the trust of the partners in the universities. With a strong track record in AAI of more than ten years, providing cloud resources to the academic community is the next step. With cloud services SWITCH aims at providing an integrated offering of network, identity and cloud services to the academic community. SWITCH aims to address specific needs of the academia such as customized billing processes and support. Also general aspects like a Swiss data location and governing law of the provider and keeping control of the data and services (governance) are important aspects that distinguish SWITCH in the role as cloud provider from international operating cloud providers. Combined with procurement services, benefits can be generated for the community in exploiting the aggregation of demand and with this economies of scale in the role of a broker as well as a provider for cloud services and infrastructure.

Q : What is the model for implementing the SWITCH cloud strategy?
SWITCH has started a pilot project with OpenStack and Ceph in 2012. Basing on the results of this project, we started building a cloud infrastructure end of 2013. The infrastructure is located in data centres of selected universities which are connected to our network. The infrastructure is operated by SWITCH engineers and as main building blocks, open source software such as OpenStack, Ceph and Ubuntu Linux are used. The first service put in production in April 2014 is a sync and share service called SWITCHdrive. It's based on ownCloud Enterprise and license agreements were worked out jointly with SURFnet and TERENA.

Commercial Cloud offerings are made available through framework agreements for the community where needed. Punctually, e.g. Office 365 is offered to members at the institutions.

Q: What is the SWITCH business model?
SWITCH provides for the initial funding for the project to develop the services. From case to case, parts of the project costs are covered through subsidies from the government, when it comes to create national services. Once the services are up and running, SWITCH aims at cost recovery and employs tariffs for their community.

Subsidies from the government can and do provide significant initial funding: In the current subsidy period (2013-2016), the government runs a program called "Scientific information: access, processing and safeguarding" where cloud infrastructures are a key area of focus. Other related areas are e.g. data management, identity management and e-publishing in science. In the first wave of financing, SWITCH has successfully applied for federal subsidies to invest in a national cloud infrastructure. This allows SWITCH to build the cloud infrastructure with more resources at a faster pace and within a framework of complementary activities.

Q: What impact has this had on your organization?

SWITCH started to implement its updated strategy in 2011. As a consequence, organisational changes were implemented. This entailed the creation of a team dedicated to advanced ICT needs (nowadays “Cloud” computing) for the academia. At that time the team partly consisted of people that worked on Grid and other international projects. In late 2013, the team laid its full focus on cloud technologies and new hiring (due to turnover) was recruited with this focus. Competencies in system and software engineering, networking, operating production infrastructures as well as identity management are needed for the successful operation of cloud services. Including the people from SWITCH’s IT operations team, the people working on the cloud infrastructure provide these competencies.

The new strategy’s core element was the conscious decision to reach out beyond central IT services in universities, to researchers, lecturers, students. Out of this, the organisational changes back in 2011 not only prepared a new team for the cloud topic. They also prepared the whole organisation for it: A new procurement team was created and cloud as a new strategic area was taken up in business development, product management, stakeholder management and sales processes.

Q: How to address technical risk?
The technical risk was addressed by gathering experience in a pilot project that had a clear scope and used a clearly defined amount of financial resources and number of people. A large enough team with a broad field of individual competencies described above is needed. On top of that training with specific know-how in cloud technologies helps to reduce technical risks.

Q: How do you address issues of scale?
With about 7 FTE on cloud infrastructures, we invested heavily in the automation of the hardware with the cloud software layer. This makes the infrastructure very scalable. Therefore we do not expect significant growth regarding people in the near future. The hardware can be procured based on the increasing usage of the cloud infrastructure. The data centre locations SWITCH currently uses provide enough reserves for the near future.

Q: Can you share any lessons learned?
Involving the future users as well as the central ICT services in the creation of new services is a key element for success. A clear positioning regarding cloud is needed and has to be clearly communicated to the stakeholders in the community. With the communication, people from the technical level up to the management level have to be addressed.

Q: What are your plans for the future?
The cloud infrastructure will be extended based on the demand of the users. The current services will continually be improved with the feedback of users and our partners in the universities. More community specific services will be added on the cloud infrastructure to complement the current IaaS and SaaS services.

A.8 Cloud services at PSNC

PSNC offers cloud computing (IaaS) and cloud storage services. We also develop, deploy and operate network connectivity, collaboration tools, data management, content management and delivery, educational systems, IoT & mobile applications, portals etc. Full information on the PSNC mission can be found at PSNC website http://www.man.poznan.pl/online/en/.

Q : What is the strategic approach to cloud for PSNC?

There is no formal, written strategy. However the real-life approach is that PSNC follows the BIY model based on in-house competence and infrastructure. We do not plan on brokering large amounts of commercial cloud resources with the exception of SaaS services, e.g. Office365 etc. as requested by our users.

Cloud services currently provided include cloud computing IaaS based on OpenStack, VMware, HyperV and KVM. These services are provided mainly within PSNC to the internal clients such as system administrators, R&D projects, software developers and testers etc. OpenStack based services are currently offered both in-house and to university partners as IaaS and SaaS models. In the future we are planning to expand the scope of software solutions offered in this way.

Campus Computing IaaS service provides the possibility to book and run virtual machines with operating systems chosen by the user. It also addresses basic cloud orchestration such as booking single and multiple collaborating VMs. Campus Computing also provides SaaS functionality, i.e. on-demand access to applications such as Matlab, Mathematica and/or graphical applications including Adobe's Photoshop etc. This enables sharing the licenses in a multi-tenant way. Work on developing the cloud platform orchestration for end-to-end management of the cloud services delivery is being conducted under B2C (Business2Cloud) and Platon/ManHA projects. Orchestrated PaaS/SaaS services are being developed, including Database-, Videoconferencing-, Digital Library-, CDN-as a Service by various PSNC departments.

Offering cloud services to our users is considered an important part of the PSNC mission and the significance of this kind of services is increasing over time. Cloud services are a natural extension and addition to the network connectivity services that we as an NREN provide to academic and research institutions since 20+ years.

Our audience includes all stakeholders mentioned above, plus research projects and infrastructures (e.g. ESFRI projects).

PSNC also collaborates with companies on building and improving quality of services, e.g. by jointly operating services or conducting relevant R&D work.

The following facts contribute to unique selling proposition of our services:

- services are provided by the trusted partner, i.e. PSNC, the PIONIER network operator and its partners in regions: MAN network operators and universities, all having long record of collaboration with end-user institutions,
- on-premises infrastructure is installed in Poland, in trusted institutions; datacenters can be physically accessed, controlled and audited;
- collaboration happens in the context of and under the Polish and EU laws;
- cloud offering is supported by documentation and training, incl. hands-on;
- cloud offering is an extension of the network connectivity service;
- users have a single point of service/access (one stop shop);
- no charges for network traffic are applied;
- there is the option to negotiate and adapt the services features and conditions.

Q : What is the model for implementing the PSNC cloud strategy?

PSNC follows the BIY model: we develop and offer cloud services based on the in-house competence, know-how and staff as well as on-premise infrastructure. Wherever possible PSNC develops services based on open source components such as OpenStack and similar. PSNC also implements its own software packages, such as e.g. National Data Storage services and tools for data replication, encryption and integrity control or cloud orchestration solution for Campus Services (originally based on Microsoft HyperV now migrated to OpenStack for better sustainability).

Commercial software is made available, e.g. through Campus Computing services. However, the strategy at PSNC is still to avoid vendor lock-in wherever possible. On the infrastructure side we use commercial packages in selected areas, where no reliable replacement has been found (e.g. TSM, VMware, etc.). We broker only *selected* services (e.g. Office365) on user demand. Our strategy prefers BIY approach and offering improved alternatives to mainstream services.

Q: What is the PSNC business model?
Depending on the funding sources available for a particular service or application area (project funds, government funding) we employ various models.

Typically the infrastructure purchase costs (the CAPEX part) are covered via the projects or national governmental funding. OPEX costs are typically also paid from project funds, however this is limited to 3 or 5 year periods in most cases.

Therefore, concerning OPEX costs two variants are possible. If we acquire funding for OPEX costs, we offer the services free of charge for the whole lifetime of a service and/or infrastructure. If the OPEX costs are not covered by external funding, we charge the users with the fraction of OPEX costs relevant to the service usage by particular users. Per-user fees are calculated based on CPU time used and RAM allocations for VMs as well as GBs or TBs used for the storage service. In more complex scenarios such as CMS as a Service, the service fees are calculated based on elements appropriate for a given application - e.g. number of digital objects handled.

Q: What impact has this had on your organization?
Development, deployment and operation of the cloud services has been incorporated into the existing departments and has become part of their usual business.

We assigned several staff members the work related to developing, deploying and operating cloud services. We fund these employees from internal sources or national and EU-funded projects.

Q: How to address technical risk?
In order to mitigate the risks that result from immature and unproven technology we develop and deploy the services gradually following best practices. Choosing and deploying a technology is decided based on the paper-based research and hands-on analysis, supported by education and training, e.g. through TF-Storage. Services deployment involves internal tests within a department and whole PSNC and roll-out to wider audience including beta tests with early adopters.

Q: How do you address issues of scale?
We estimate resources needed to address future demands based on the observations of current resources usage and dynamics of the demand. This is complemented by the dialog with the end-users. We also take into account the overall IT trends documented by IT market analyst and data acquired from other academic providers.

We purchase the equipment mainly on a project basis. Planning covers 3-5 years since purchase. We have limited capacity to dynamically adapt to the changing demands between the funding cycles therefore we typically calculate the spare capacity into the purchases, which enables addressing the dynamically arising needs.

Part of the strategy is also that we address the most challenging use cases with the hardware we currently purchase and move the ageing hardware such as computing servers or storage systems towards the less demanding applications.

Q: Can you share any lessons learned?
High-level lessons:

- Building and offering the cloud services is not only a technical issue. Organisational changes may be needed including building a competence, organizing a team dedicated to serving cloud users as well as working out elastic infrastructure funding models and developing a service fee schemes.
- In the cloud era, users tend to expect more flexibility on the provider side than before. This is a technical an organizational challenge for NRENs. On the other hand, if we address these expectations properly, our flexibility will contribute to advantages of our offering vs the commercial providers.
- It is hard to compete with commercials on the general purpose, basic services such as documents editing software etc. For these reasons we agreed to broker Office365. We will also consider broker other services if the needs arise. From the other hand, NRENs services may provide unique important added values, e.g. better data security, trust, etc. that might be crucial in the applications involving processing, storage and preservation of sensitive data.
- The low level services such as IaaS addresses the needs of these end-users, who are capable of building the high-level, specific service by themselves.
- Developing and offering the services targeted to large audience such as general purpose application access in cloud and/or personal storage or sync&share systems require a different approach than providing pure IaaS or flat storage solutions. The more high-level is the service, the more work is needed on ensuring user-friendliness of the interface and the simplicity of the enrollment process (federated Id systems might be helpful at this stage).
- We might be unable to offer cloud services if we weren't offering the network connectivity. The fact that we are already providing the network opens the doors for providing the other services. Also the fact that we do not charge the users for the network traffic related to usage of our services constitutes an advantage when compared to commercial systems.
- The fact that we are project-funded requires a careful capacity planning. It also requires working out the approach that ensures that OPEX costs are covered after the project lifetime. This may lead to charging the users with the fraction of OPEX. On the other hand, we can offer users the flat rate based cost fee schemes (e.g. the yearly price of storage capacity) that are easier to handle by them, as they typically plan the costs on yearly basis.

Q: What are your plans for the future?

Further development of 'golden alternatives' to mainstream services. Rollout of the cloud computing platform and solutions for secure data storage, access and sharing.

Collaboration with other NRENs on improving the capacity and reliability of our services, possibly based on exchanging the cloud resources such as CPUs, memory and/or storage capacity, I/O capabilities etc.

A.9 Cloud services at CESNET

CESNET currently provides a relatively broad portfolio of services which can be understood as "cloud" services. Especially computing clouds and grids (which are focused on scientific applications), data storage (represented mainly by ownCloud), VC services and so on.

Q : What is the strategic approach to cloud for CESNET?

CESNET doesn't yet have a strategy document for cloud adoption, but we are considering making one in the future. We believe that providing cloud services is currently one of the key areas for NRENs. This corresponds to the user demand for these services.

We see the main target audience in IT departments of Universities and Research Organizations. Providing services directly for end users (i.e. students) is very complex business and CESNET does not have adequate resources.

Q : What is your current implementation model?
Our existing cloud services are provided completely as an in-house solution based mainly on open-source components. We prefer this model.

However, we are currently considering providing Microsoft Office365 hybrid cloud, which is of course based on the very commercial software.

Brokering of cloud services offered by external providers is still in phase of considerations. We believe that such activity could be beneficial for our users (mainly because of potential savings from scale and unification of services) but no concrete steps was taken yet.

Q: What is the CESNET business model?
All currently operated cloud services are provided to users within a single fee for access to the e-infrastructure. There is no special fee for specific cloud services used by particular users. Most investment expenses are covered by national or international projects through targeted grants to upgrade the e-infrastructure capacity (especially European Structural Funds). The second largest source of financing are direct payments from users for access to the e-infrastructure.

Q: What impact has this had on your organization?
Providing new services brings new nontrivial financial expenses (both OPEX and CAPEX). It also brings a commitment to users for the future, that CESNET will provide services for a certain period in a defined quality. And of course demand for new staff - in connection with the launch of new cloud services, CESNET must recruit experts for new technologies which already wasn't operating and has no experience with them (especially Microsoft technology).

Q: How do you address technical risk?
Technical risks are treated particularly by precise testing and collaboration with technology partners.

Q: How do you address issues of scale?
We carry out preliminary surveys (relevance of new service, number of potential users, anticipated storage requirements, etc.). We also perform a detailed analysis of system utilization for existing services and on this basis we plan a possible upgrade of hardware resources.

Q: Can you share any lessons learned?
The introduction of new cloud services is quite challenging activity. Cloud services are currently a modern topic, everybody talks about clouds and all are interested in them. However, when users should actually start using a new cloud services in practice, they often realized that those are not suitable for them, they do not trust their providers for security reasons, services are too expensive for them etc.

Q: What are your plans for the future?
We are planning to start Microsoft Office365 hybrid cloud service in a relatively short future. But we are still in preparation phase – pilot test is currently running.

We are also considering some form of cloud service brokerage but it is just an intent at the moment.

Q: How are you working with the GÉANT SA7 cloud activity and how do you benefit from this?
We are working mainly on launching a test deployment of hybrid cloud Microsoft Office365 within the GN3+-SA7-T6.

A.10 Google Apps for Education at the University of Groningen

“It's a good product and people like using it”.

In May 2014, the University of Groningen migrated its students and staff to Google Apps for Education. As a result, all students and staff now have access to an account with various functionalities, such as email (Gmail), a calendar (Google Calendar), chat (Google Talk), documents (Google Drive) and web pages (Google Sites). The university is also set to introduce SURFdrive in the short term in order to facilitate the secure sharing of data.

Q: Why opt for the cloud?
The University of Groningen fully supports the ‘cloud first’ philosophy. “Collaboration environments are becoming increasingly cloud-based. These cloud services offer far more functionalities at lower prices. We expect this trend to really take off in the years ahead”, explains Haije Wind, technical director (CTO) at the University of Groningen.

The transition was also optimally timed in practical terms. The current email and calendar functions were due for replacement, and faculty staff were demanding greater functionality.

Q: Why opt for Google Apps for Education?
Various cloud environments were analysed in preparation for the definitive selection procedure. For example, the university considered Microsoft Office 365 and Zimbra. These packages did not meet the relevant requirements, partly due to a lack of knowledge on Microsoft ICT within the University of Groningen, and the immaturity of the Zimbra environment.

It didn't take long to reach consensus on Google Apps for Education. Google offers a number of crucial advantages over the various alternatives. For example, Google offers an open system with many functionalities that suit the University of Groningen's specific needs. Google had also already established a firm foothold in the education market at the time the decision was made, whereas Microsoft has traditionally serviced the business market. Google is an industry leader in terms of cloud development and a strong innovator; new functionalities are constantly being added. Google also has an existing connection with SURFconext and can be easily linked to other environments such as Blackboard.

Despite our faith in Google Apps for Education, we also prepared an exit strategy: how easily could we transfer the data back to the old system if the environment didn't prove to be suitable for the University of Groningen?

Q: Why opt for SURFdrive?
The secure sharing of data is important, especially to researchers. Google doesn't necessarily offer this functionality, prompting the university to seek an alternative for data sharing via Google. This aspect was essential to the successful roll-out of Google Apps for Education at the University of Groningen. The institution initially used its own service: EduShare. The university started migration to SURFdrive on 1 January 2015.

Q: How did you organise the migration process?
“We involved our staff in the process from the outset. We developed a campaign which proved crucial to the success of the implementation process”, explains project leader Sander Liemberg. We focused attention on the migration in various ways: from practical information online to boxes with sweets and Google chocolate informing users that the migration was about to take place. We made sure no one could remain unaware of the transition.

In more substantive terms, we held a great deal of meetings with users to find out whether Google Apps for Education was genuinely usable and offered a real functional improvement. We also organised walk-in sessions and training courses. These meetings and walk-in sessions offered an ideal opportunity to inform our staff and enthuse them about the migration process. A number of challenges also came to light. For example: how do you approach the delegated calendars used by secretaries, which tend to get confusing when used in practice.

Despite these points for attention, we concluded that Google does offer genuine added value. For example, everyone can now access their calendar from any location and device. The new system also makes it easy to share calendars, and universal use of the same functionality allows employees and students to schedule appointments and make arrangements.

A pilot project was conducted prior to the launch of Google Apps for Education. When this project proved successful, Google was rolled out on a large scale. Students - generally familiar with Google solutions - were first to make the transition. Staff members migrated to Google email and calendars about one year later. The University of Groningen relied heavily on the support of its staff members and service desk over the course of the large-scale implementation process.

Q: How did you deal with the resistance?
The technical aspects didn't present that much of a problem, but we had to spend a great deal of effort getting our students and employees on board. After all, “change is always difficult, and the project was under intense scrutiny.”

Just after we'd decided to use Google Apps, the news media started to report stories on data leaks. “Everyone now knows about WikiLeaks, and you really have to defend the decision to use the cloud”, Haije Wind explains.

In response, the University of Groningen focused on explaining its choices. It also highlighted the benefits: the improved functionalities outweigh any disadvantages. Efforts were also made to emphasise that the University of Groningen's contractual agreement with Google is not subject to the same terms and conditions as standard consumer contracts. For example, the business contract stipulates that the University of Groningen will retain ownership of all data. Furthermore, no Google ads will be displayed in the University of Groningen environment.

The University of Groningen also genuinely listened to opponents of the solution. Partly in response to their concerns, EduShare (soon to be followed by SURFdrive) was introduced as an alternative for data sharing via Google. A campaign was also conducted in order to address and assuage the various concerns and objections.

Our efforts to provide further explanation and address user needs proved successful: the new system is now almost universally supported within the university. One faculty initially refused to make the transition to Gmail, but is now expected to do so in the short term. The option of encryption, digital signing and combination with SURFdrive as an alternative for data sharing are all important in this regard.

Q: What did the transition cost and yield in financial terms?
The old email and calendar system was due for replacement, and investments were inevitable. Our decision to opt for Google Apps for Education yielded immediate financial savings, eliminating the need to purchase a new system and software licence.

However, we did incur some additional costs in aid of process supervision and the hiring of external capacity. Our current functional management system will also remain in place, so that aspect doesn't offer any potential for savings.

The core team assigned to the project was made up of around eight people. We also deployed a total of ten technicians. We built all the various interfaces, such as the plug-in for the university portal, in-house.

Expenditures also included the migration tool, which was built by an external party. This tool allowed employees to migrate data from the old email system to Google.

The process put a great deal of strain on our support and service desk. We resolved the problem by bringing in external staff members. A staff of around twenty people were deployed over a two-month period. We also deployed student assistants to assist employees with the migration process on-site. These measures helped us to manage costs more effectively.

Q: What sort of technical issues came up over the course of the process?
As Sander Liemberg and Haije Wind explain, the process didn't present any technical problems. However, we did underestimate the aspect of data migration. Copying data from one environment to another proved to be extremely time-consuming. This delay was attributable to Google, and the University of Groningen was unable to speed up the process. This caused a certain amount of commotion, as the number of people that could simultaneously migrate their data became limited. It also necessitated a considerable amount of supervision.

The migration tool developed by the University of Groningen initially suffered from some bugs. Despite the inconvenience, we didn't lose any emails and managed to resolve the issues quickly. Google has since developed its own migration tool. Sander Liemberg emphasises that a more effective migration process would help speed up the adoption process. The university stores duplicate copies of all emails in order to facilitate disaster recovery. This low-cost solution helps set everyone's mind at ease.

Q: What sort of legal issues came up over the course of the process?
We had to take quite a few legal measures. For example, all contracts with Google had to meet the requirements applied by Dutch universities. SURF played an important role in this regard, as Wind and Liemberg explain. SURF arranged meetings that gave the University of Groningen an opportunity to literally sit at the table with Google in order to ask questions, negotiate issues such as Safe Harbour principles and Google ads, and conclude the definitive contractual agreements.

“There are still a lot of unknowns in terms of the legal aspects. Ensuring legal compliance is a constant challenge. Amongst other measures, we've worked to ensure accountability by allowing audits and other forms of monitoring. Google also has to offer insight into its security measures and report any hacks", Haije Wind explains. Despite being a first for Google, the company proved to be open to these measures which were suggested and coordinated by SURF. The ability to log in via the federation is regarded as a major advantage. This eliminates the need to hand over any passwords to Google, which was one of the university's security requirements.

The outcome

Our users are extremely satisfied and are now requesting access to other Google Apps for education functionalities. These requirements will be addressed over the course of a follow-up project. Project leader Sander Liemberg views these additional wishes as a promising sign: “Apparently, Gmail and Calendar are now well integrated into the day-to-day workflow, and people are starting to see the possibilities.”

Technical director Wind is most satisfied with the environment itself: “It's a good product and people like using it. We're not getting any complaints”. “Google is very stable. It's an appealing, fresh environment that works on any device in any location. That's obviously a major advantage”, Liemberg adds.

The university is seeking to extend its contract with Google for the coming four-year period. The contract will be automatically extended by two years, but this period may be exceeded.

The Google train

Google is a dynamic company. New functionalities are constantly being added ("we're getting on board the Google train"). The University of Groningen will be assessing their usability in consultation with users during the follow-up stage. For instance, Google Groups may help streamline the group collaboration process while Blackboard could be integrated into the current system, making it easier to display study timetables. The university will also be using Google Hangouts on a large scale for the first time, as part of a Massive Open Online Class (MOOC).

Specific lessons and advice for other institutions

- An effective plan for internal and external communications and interactions with the media is crucial.
- Make sure to develop an exit strategy: how quickly and easily can data be retrieved from the system if a decision is made to switch to another solution?
- We placed a great deal of emphasis on creating awareness (posters, sweets, Google chocolate) and providing support (online by means of manuals and offline by means of walk-in sessions, training courses and a service desk). This proved to be crucial.
- We also listened closely to the wishes and arguments of opponents. We could then incorporate their concerns, which benefited the adoption process.
- The data migration process took longer than expected. This should be factored into planning schedules and communications to users.
- Students tend to adopt new solutions more readily than employees. Starting the process with students proved to be an effective measure.

There's a solution for every potential objection: SURFdrive for secure data sharing, encryption, tailor-made agreements with Google, etc.

A.11 Collaboration services at RENATER

We don't offer a cloud IaaS service at the present time. However, what we do offer is various collaboration services such as PARTAGE, a mail service, and RENDEZ-VOUS.

Q : What is the strategic approach to cloud for RENATER?
We haven't yet defined a real cloud IaaS strategy for the moment, we are still working on it! We have started a study about the feasibility of a sync/share cloud storage service (i.e. a Dropbox-like service) for research and academic organizations.

RENDEZ-VOUS is another very good candidate as in essence has been designed to work on a cloud model. Up to now there was no good software that could provide a cost effective and thus affordable WebConferencing service. The software is OpenSource so that prevents vendor lock-in.

Q : What is your current implementation model?
The software that powers RENDEZ-VOUS is JITSI, which is extensible and provides a tremendous opportunity to fulfil most of our user's requirements, especially privacy. It is inherently designed to leverage Cloud infrastructure.

In addition, our collaboration in SA7 with other NRENs allowed us to reach a scale that has never been achieved before. The numbers depict a promising success and encourage us to keep the development in this direction. For the record we have ~5000 H323 conferences per month. With RENDEZ-VOUS pilot we reached 14000 conferences per month involving 30000 connected users!

Q: What is the RENATER business model?
Such services, if we choose to provide them, would be in a full cost recovery model.

Q: What impact has this had on your organization?
As stated before, we achieved and unprecedented scale with this service. Visibility is then also increased. In that context, more man power would be needed.

Q: How do you address technical risk?
The software is open source, in that sense a technical risk is only to rely on the developers behind JITSI. This is currently addressed, a lot of effort is being put in to studying the code.

Q: How do you address issues of scale?
RENDEZ-VOUS is addressing the scaling problem by leveraging various available clouds. In essence, the application is relaying the creation of a room in the proper VM conforming to various rules/constraints. These constraints can be the available bandwidth, the CPU load, the memory consumption and even the geo-location of the VM.

Q: Can you share any lessons learned?
Deploying cloud services is a great challenge. The commercial companies often offer a free or cheap service for end users who subscribe individually and the academic organizations are often unable or unwilling to evaluate the full cost of their in-house solutions. So, our offers are often considered as too expensive.

With RENDEZ-VOUS we will strive to push the scalability limit in order to make WebConferencing available to every single person in the European R&E community. One thing though is to put the focus on usability, privacy and simplicity. In that context, Innovation is possible only if adoption is easy.

Q: What are your plans for the future?
RENDEZ-VOUS is the stepping stone to various application that uses WebConferencing. However, the adoption of RENDEZ-VOUS is the first challenge in order to move forward. One of the key issues that has been raised is the integration with the existing legacy unified communication system.

Q: How are you working with the GÉANT SA7 cloud activity and how do you benefit from this.
Collaboration through SA7 was a unique opportunity:

- To push the scaling limit of RENDEZ-VOUS at another level
- To test the software in various condition (sofware and geographic)
- To get valuable feedback from different users belong to different culture
- To work on an agile and flexible model

A.12 A survey of cloud service transition cases at selected universities in the Czech Republic

This story describes the results of a survey carried out on two Czech universities (Czech Technical University Engineering - **ČVUT**, University of Pardubice - **UP**), which cooperate with CESNET within the project activities GN3+ (especially on preparing a pilot project of the Office 365 hybrid cloud). The aim of the survey was to determine the attitudes, experiences and future plans regarding the deployment of cloud services at these universities. Practical experiences in this area may serve as a valuable basis to other universities during the implementation of cloud services.

Basic information about the selected universities (the numbers are approximate estimates):

University	Employees no.	Students no.	Equipment
ČVUT	4500	20000	10 thousand PC (plus unspecified number of terminals)
UP	1200	10000	3300 PC (plus 600 virtual desktops)

As part of the survey the following set of questions was submitted to the IT departments of selected universities, which were aimed at their attitudes and experiences related to the process of implementing cloud services type in their specific environment. Answers to the questions were discussed in detail with competent managers of these departments:

1. Which cloud services are you already using today?
2. Which cloud services are you planning to use in the future?
3. What is your organization strategy for cloud transition?
4. What are the major problems your IT is facing today?
5. What are the plans and needs of your IT future (transition strategy for cloud services, roadmap steps, etc.)?
6. What services (additional) may be CESNET able to offer in the future and what other help you expect of CESNET in the field of IT and cloud services?
7. Can you please briefly describe the procedure and possibly also problems during your transition to currently used cloud services?
8. Can you please briefly describe your experience with the use and implementation of cloud services (results and lessons learned from the implementation process from the perspective of both suppliers and users)?
9. What are the reasons and motivations of transition to new cloud services?
10. What are your expectations of CESNET in relation to the needs of the University in the field of IT services (including new cloud types)?

For the questions we obtained the following responses:

Cloud services currently used (Q 1.)

ČVUT: We are currently using MS Office 365 with connection to Active Directory (incl. OneDrive to store and share data); for storage some users use ownCloud provided by CESNET, however, they mostly use a commercial solutions like Dropbox, Apple iCloud, Google Drive and others. For e-mail, some faculties use Gmail, other Office 365 Exchange - usually each faculty has its solution (Novell GroupWise, MS Exchange, Linux Open source solutions...). To create and share documents, faculties use MS Office 365. In terms of computing services (IaaS) local computing centers are used, and exceptionally users (groups) cooperate with computing centers abroad (USA, EU ...).

UP: We are currently using MS Office 365 with connection to Active Directory (currently in the phase of gradual migration and testing); for file storage some users are using either ownCloud provided by CESNET or MS Office 365 OneDrive. For e-mail – employees are currently in the state of hybrid solution - the majority uses the local MS Exchange, the rest is using Office 365; students are using Gmail for a long time (however, due to the fact that Google is changing the internal API the university IT is also considering transition of students to MS Office 365). Some users (staff and students) also use FileSender cloud service provided by CESNET for sending large amounts of data. For calculations is also marginally used MetaCenter cloud service provided by CESNET - but we also own computing resources that cover most of our computing needs.

Future planned cloud services (Q 2.)

ČVUT: In the area of data storage and sharing we plan to reinforce the use of Data Storage cloud service provided by CESNET and further develop (expand) existing solutions, especially solutions based on MS Office 365 (incl. involvement in the planned hybrid cloud solution by CESNET). In the area of computer services we will continue to develop our own data centre and cooperation with foreign data centres.

UP: There are two different possible scenarios for further university IT development (decision must be made soon) - either remain at current hybrid solution (local vs. public cloud system) or use completely hosted cloud MS Office 365 (incl. the planned use of the hybrid cloud by CESNET).

Transition strategy for cloud services (Q 3.)

ČVUT: There is no approved central strategy of transition to cloud solutions, but it is evolving in line with current user needs and opportunities (we explore and evaluate various solution scenarios).

UP: The strategy for future cloud-based solutions (services) development will depend a lot on the assessment and answer important questions related to the legal aspects of a legislative framework. Legislative aspects must be resolved in order to convince the leadership of the university and faculties for usage of cloud based services at all. In particular, the assessment of safety and credibility to store data outside the organization (ensuring the protection of personal data, etc.).

Current major problems for university IT (Q 4.)

ČVUT: Major problems of university IT currently are: lack of funds to cover all requirements from users and unreasonable expectations of users that do not meet current capabilities (e.g. on continuous customer support 24/7), followed by excessive organization (academic) freedom within the university. Such freedom means practical difficulties for enforcing any central solution (incl. non-centrally prescribed rules). Finally there is a problem caused by promotion of individual requirements for the solution of individual faculties or departments tailored for their employee needs without agreement with each other.

UP: The current IT problems at university are (rather non-technical) as follows: under-funding and sustainability of technology, wages of people staffing deficit (in terms of ensuring 100% substitutability), complications resulting from the application of legal standards (especially the Public Procurement Act) on purchases of equipment and technologies. Problems occur especially in relation to the future sustainability of acquired infrastructure using financial resources from EU Structural Funds – it isn't easy to decide whether in future to go further through outsourcing or renewing the infrastructure (demanding solution - for finance and human resources). In addition, occasionally we encounter compatibility problems of individual software solutions (e.g. Office 365 is not compatible with old versions of MS Office 2003, which some users do not want to leave and we can't force them to do it; moreover it's connected with demands for user training). This of course means a non-unified solution for administration.

Future plans and needs of the university in the field of IT (Q 5.)

ČVUT: In terms of future plans and needs in the field of IT university is planning gradual unification and building a unified solutions based on the identified needs of users and the agreement with the management of faculties and universities. The aim is to ensure the effectiveness of a defined quality of service.

UP: From the perspective of a migration strategy of the university to cloud services it is necessary to carry out especially the following steps:

- Identify the real needs of the employees and students to cloud services.
- Develop internal policies for cloud services.
- Ensure legislative certainty in the use of these services.
- Discuss and approve the use of cloud services with the university management.
- Verify the technical possibilities and provision (financial difficulty).

In so-called critical applications (Study and economic agenda) there is no reason to shift resources outside the university. At the same time we are preparing to use Data Storage cloud services by CESNET, for such applications that don't require fast access to data (storing photographs and video archive). In the future, the situation may also change for some other services (due to termination of support for certain systems or the necessity of renewal HW etc.), and then we will consider how to proceed (whether to go to cloud services or not etc.).

Services and any other assistance that CESNET might in the future offer to the university (Q 6.)

ČVUT: We expect from CESNET such services (e.g. in the area of storage and archiving of data), which represent a significant added value to the university and such services must be provided with high availability. CESNET might also play a significant role in coordinating central purchase of common SW, HW, licenses etc. A solution that would allow dynamic sharing of licenses among universities, including virtualization software (e.g. VMWare and others).

UP: CESNET should in the future be able to assist in uniting approach of universities, in technological, legislative and implementation areas, as well as in the sharing of experience, best practice and better informing at different management levels (e.g. at the level of university managements etc.). At the same time the CESNET is expected to fulfill the role of national coordinator for future EU Structural Funds projects. This should ensure sustainability of such projects thanks to central shopping HW, SW, licenses and virtualization systems. This approach might allow achieving better conditions for the acquisition and purchase of services than what can be achieved when the individual universities or faculties negotiate with suppliers.

Procedure and eventual complications of transitioning to cloud services currently used by the university (Q 7.)

ČVUT: When introducing new cloud services it was necessary to keep roughly the following:

1. Enforce the basic idea of transition to cloud service and emphasize its advantages.
2. Agreement on a unified solution.
3. Preparation of implementation (incl. training IT personnel, negotiations with suppliers etc.).
4. Process of implementation (installation with ensuring of providing a support from the vendor on the required level of quality).
5. Migration of users to the new system and solving problems associated with it.

UP: The key findings from the transition to a new cloud-based solutions:

1. From the technical point of view it's all about ensuring reliability and 100% availability of all services (hence the cloud). Therefore even the test operation of any solution shall be at full operation capability and must therefore be properly prepared.
2. Simultaneously with the introduction of new solutions there must be user training, which we can't impose, but users themselves must first see the need and usefulness of the new solution thus training on the new system (both must be attractive enough for them). Users are accustomed to have all the necessary information (trailers etc.) on the university intranet in advance to the training.

Description of the university's experience with the use of cloud services and lessons learned from the process of their implementation. (Q 8.)

ČVUT: Experience and lessons learned from the process of implementing a new cloud solution:

- During the implementation process of the transition to the new cloud services it is very important to have the holder of the main ideas who would over a longer time horizon, patiently and persistently create a suitable environment tailored to user needs.
- It is also important PR-preparation of users in advance and explanation of what we want to achieve with new solution.
- The success of the process is also inseparably connected with the planning discipline itself in the context of the subsequent operating costs – there is a need for long term planning, especially in terms of sustainability.

UP: Basic lessons learned from the cloud implementation process:

- It is necessary to thoroughly analyze the environment and research needs on the part of universities, especially by the provider of cloud services. Simultaneously it is also important to find users (those who are trusted by the others and also who may bring some new ideas to current solution) for the implementation and testing of new services (they must be drawn in an appropriate manner during the implementation process).
- It is also necessary to overcome user mistrust and train them.
- When introducing new services is a very important to have an implementation partner who is at the appropriate level, in terms of know-how and experience.

University's motivation and reasons for transition to cloud services (Q 9.)

ČVUT: Motivation for the transition to cloud services was associated with the expectation of a greater degree of cooperation among users across the university. At the same time we needed to consolidate identity management in the area of data storage and sharing, planning, cooperation etc.

UP: Reasons for migration to new cloud services are essentially two:

- HW limitations and costly management of local systems (with a view to reducing labor and management connected to administration of information system).
- Technological reasons - general technologic progress and the need called Unified Communications (involving mobile devices, etc.) drives the transition to new solutions using the cloud.

University's expectations of CESNET in connection with the IT service needs (Q 10)

ČVUT: Expectations of the University to CESNET in the area of IT:

- The main expectation is a greater degree of service guarantee (even at the cost of additional charges, e.g. for extra availability etc.).
- It must be also clear the added value of services provided by CESNET - from the perspective of the university goes especially simple and reliable access to IT services. At the same time, these services must reflect the real needs of the user community.
- Cloud services such as IaaS may also be interesting, but they must be provided with certain guarantees.
- It could be interesting to have a comprehensive data archiving service (within the meaning of the electronic library of all data university and faculty agenda).
- Another possible benefit would be if CESNET acted as the authority for electronic signatures and in terms of e-government (data boxes etc.).
- The possible benefits include provision of e-learning services (provided with effective support, i.e. with the indicative ready templates functioning and usage scenarios).

UP: Ideas for cooperation with CESNET:

- From the perspective of the university is required for CESNET to play the role of both the national coordinator and provider of unique services, but also in the field of professional guarantor of these services.
- PR-role of CESNET is also important, especially the need to raise awareness of university management about the role of CESNET and the benefits of its offered services (and those resulting from cooperation of universities with CESNET).

Conclusions

1. The survey shows that universities are aware of the usefulness and a significant contribution (added value) transition to a cloud service model (selected universities represent a small but representative sample of Czech public universities).
2. The survey outcomes also suggests that universities continue to have interest in cooperation with CESNET, among others in the field of cloud services. However their requirements emphases high availability and guaranteed level of provision such services.
3. The most important lesson from the cloud transition on universities is the necessity of a thorough analysis of the school environment, awareness and familiarity with the specific user community. Users must be familiar with new service benefits. User training is necessary and also the co-operation with supplier (implementation partner) and providing of the support should be on required qualitative level.
4. Before using the cloud services universities need clarification of issues related to data security and legislative conditions of data storage outside the organization.
5. Finally, university management and user community must be also convinced about the effectiveness and economic and organizational benefits of the transition to a new model of IT (cloud) services (the need for uniform and unified solution).

Appendix B References

[1] Dr Diane McDonald, Archie MacDonald & Caroline Breslin, "Final report from the JISC Review of the Environmental and Organisational Implications of Cloud Computing in Higher and Further Education", University of Strathclyde, Glasgow, May 2010. http://www.jisc.ac.uk/media/documents/programmes/greeningict/cloudstudyreport.pdf

[2] Dr Max Hammond, Dr Rob Hawtin, Dr Lee Gillam, Prof Charles Oppenheim, "Cloud computing for research – final report", Curtis+Cartwright Consulting ltd, JISC project, June, 2010. http://www.jisc.ac.uk/media/documents/programmes/research_infrastructure/cc421d007-1.0%20cloud_computing_for_research_final_report.pdf

[3] Xiaoyu Chen, Gary B. Wills, Lester Gilbert, David Bacigalupo, „Using Cloud for Research: a Technical Review", School of Electronic and Computer Science, University of Southampton, June, 2010. http://tecires.ecs.soton.ac.uk/docs/TeciRes_Technical_Report.pdf

[4] Nicole Convery, "Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud", Department of Information Studies, Aberystwyth University, August, 2010.

[5] e-IRG, "Cloud Computing for research and science: a holistic overview, policy, and recommendations", October 2012, http://www.e-irg.eu/images/stories/dissemination/e-irg_cloud_computing_paper_v.final.pdf

[6] Maria Spinola, "An Essential Guide to Possibilities and Risks of Cloud Computing", June, 2010, http://www.mariaspinola.com/whitepapers/An_Essential_Guide_to_Possibilities_and_Risks_of_Cloud_Computing-A_Pragmatic_Effective_and_Hype_Free_Approach_For_Strategic_Enterprise_Decision_Making.pdf

[7] Daniele Catteddu, Giles Hogben, „Cloud Computing - Benefits, Risks And Recommendations for Information Security", European Network and Information Security Agency (ENISA), 2009.

[8] Cloud Computing Use Cases White Paper, Cloud Computing Use Case Discussion Group, June 2010. http://www.cloudusecases.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.odt

[9] Jim Reavis, Daniele Catteddu, "Cloud Security Alliance Contribution to the European Commission Strategy on Cloud Computing", November, 2011, https://cloudsecurityalliance.org/wp-content/uploads/2011/11/CSA_EU_Response_Final.pdf

[10] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, v3.0", 2011, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[11] Michael Hogan, Fang Liu, Annie Sokol, Jin Tong "NIST Cloud Computing Standards Roadmap, Special Publication 500-291, July 2011, http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Jul5A.pdf

[12] Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese, Paul Hopkins, "The Cloud - Understanding the Security, Privacy and Trust Challenges", November, 2010. http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf

[13] GN3plus, Support to clouds Service Activity, "MS7.1.1 Cloud Assessment Document - Questionnaire Response Summary", August, 2013: https://intranet.GÉANT.net/SA7/T1/SA7%20Task%201%20documents/MS94_MS7%201%201_Cloud-Assessment-Document.pdf

[14] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe, Brussels, 27.9.2012. http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-529-EN-F1-1.Pdf

[15] https://okeanos.grnet.gr/

[16] http://code.grnet.gr/projects/{synnefo, pithos, astakos, aquarium}

[17] Sage A. Weil, Andrew W. Leung, Scott A. Brandt, Carlos Maltzahn. RADOS: A Fast, Scalable, and Reliable Storage Service for Petabyte-scale Storage Clusters. Petascale Data Storage Workshop SC07, November, 2007.