28-02-2020

GÉANT Cloud Strategy Guide for Institutions

Contents

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

1 Introduction

Universities and research institutions have a strong demand for IT-supported research and education, heavily investing in computing facilities, equipment and additional overheads to support their operation. With the evolution of technology, many commodity and subject-specific services have changed from traditional form to online, provided through cloud technology.

The Digital Agenda for Europe [DigitalAgenda] underlines the need to develop an EU-wide strategy in order to adopt cloud computing, while the e-Infrastructure Reflection Group (e-IRG), in its study *Cloud Computing for research and science: a holistic overview, policy, and recommendations* [e-IRG_CloudComputing], recommends establishing and promoting the necessary policy, rules and legal framework at national and European level.

GÉANT, the leading collaboration on e-infrastructure and services for research and education [GÉANT], and National Research and Education Networks (NRENs) help the European R&E community to explore the use of cloud services. In that process, a strategic approach is essential to ensure successful cloud services adoption. This document aims to help policymakers navigate through the complexity of the cloud services domain in order to define a clear strategy towards cloud services provisioning.

The proposed methodology for developing a cloud strategy has three stages:

1. **Strategic analysis** – The initial stage is to conduct an extensive analysis of the needs of both the institution and its users, who may have relatively generic and/or highly specific requirements. The analysis stage should also address the potential benefits of cloud computing, as well as barriers to the adoption of cloud services.

2. **Strategy synthesis** – The next stage is to use the outcome of the analysis stage as a foundation to identify strategic goals for those cloud services that are consistent with the organisation's overall strategy and vision. The identification of strategic goals should address the requirements of stakeholders and identify what specific services are required, the appropriate service delivery model (SaaS, PaaS, IaaS) and the deployment model (public, private, community, hybrid). The work of GÉANT and the NRENs has demonstrated that deciding the role of the institution and the appropriate level of involvement in the delivery of cloud services is key. This role can vary from a fully internal develop, build and deploy model to the opposite extreme of a fully external managed or brokered service using an external cloud provider and its infrastructure and resources.

3. **Strategy implementation** – The final stage is to focus clearly on how the service(s) will be implemented. It should provide a clear roadmap that defines all the major activities and resources needed to achieve the strategic goals with acceptable cost, time and effort. The implementation should consider the risk assessment and management as well as the organisational impact, such as the requirement for new skills, resources or activities. Finally, the institution needs to consider service branding and how it positions and communicates the new cloud service(s) with users.

The remaining sections of this document identify and discuss the most important considerations that should be taken into account during each of these three stages in developing a cloud strategy for

research and education institutions. More detailed information is provided in *NREN Cloud Strategy Guide* [GN_CloudStrategyGuide], while other useful information can be found in *Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud*, *Final Report from the Review of the Environmental and Organisational Implications of Cloud Computing in Higher and Further Education* and *NIST Cloud Computing Standards Roadmap* [CloudToolkit; CloudImplications; CloudStdsRoadmap].

2 Strategic Analysis

In the strategic analysis stage, a wide range of information must be gathered and analysed in order to define strategic goals. This analytical process should involve the following steps:

- Understand the values of key stakeholders (individual users, departments, funding bodies).
- Analyse:
  - User business processes, needs and demands in relation to the potential of cloud services.
  - Drivers and benefits of using various cloud services from the end-user perspective.
  - Barriers, risks and other issues that need to be resolved in order to exploit the benefits.
  - External influences, consisting of many aspects, such as political, economic, social, technological, legal and environmental.
  - Internal influences, addressing the institution's capabilities to implement the strategy, including internal strengths and weaknesses.

For successful adoption of cloud services, the first three analysis areas, addressing the user perspective, are crucial, and are described in the rest of this section.

2.1 User Needs and Demands

The user community in a typical institution will generate a demand for general computing, network, storage and application resources to meet common requirements such as email, office productivity applications, videoconferencing, storage, backup, file sharing, customer relationship management (CRM), database hosting, web hosting and other typical needs common to most organisations.

In the research and education community there is also a significant additional need for more specialised computing and storage resources, driven by use cases specific to the nature of the work carried out by the sector.

Table 2.1 below summarises the general and sector-specific computing requirements of a research and education community.

General computing	R&E computing
Requirements are common to many organisations	Requirements are specific (e.g. performance)
Load varies on daily and weekly cycles (e.g. low night use)	Load is high during scientific experiments that can take weeks
Availability may be critical for business normal functions	Availability is not usually critical (experiments can be restarted a day later or in the near future)

General computing	R&E computing
Long-term predictable use cases (stable configuration and requirements)	Configurations may vary dramatically according to the experiments being run

Table 2.1: General and sector-specific computing requirements of an R&E user community

These two user environments have very different computing requirements, and possibly different solutions, so in defining a strategy for cloud services, it is important to consider both sets of needs.

2.2 Advantages and Benefits

The potential advantages and benefits of using cloud computing are outlined below. The list gives the generally accepted reasons for adopting cloud computing services, and should be further analysed in relation to the specific business processes and use cases in the research and education context.

- **Cost-effective** – One of the most attractive benefits of cloud computing is the potential for significantly reducing capital investment requirements. It does not necessarily mean that the total cost will be reduced in the long term, as that depends on many other factors and the method of usage, such as pay-as-you-go and on-demand payment models. Nevertheless, the financing is well-balanced, moving the funding from capital investment to operational cost (from capex to opex). The overall cost-effectiveness should also be analysed in a wider context, taking into account other benefits as well.
- **Easy and fast deployment (more agility)** – Researchers can focus more efficiently on research and scientific activities and innovation, without having to deal with system, network and security settings to run their experiments, while students can also easily and quickly obtain the resources to complete their educational activities and release them once the activity is complete.
- **More flexibility and scalability** – The capacity required by research projects and scientific experiments is not always predictable. In a cloud-based environment this is not a concern, as users can easily increase and decrease capacity or just use what they need when they need it and pay according to the usage.
- **Ease of use and mobility** – Cloud computing offers simplified usage and universal access from any location with Internet connectivity, resulting in improved productivity in the areas of science and research, and more efficient learning environments.
- **Improved research collaboration** – With improved accessibility and data sharing in real time from any location, collaboration is improved both internally, within the institution, and externally, with other local or international partners, such as a pan-European project consortium.
- **Business continuity** – Instead of institutions investing in their own disaster-recovery facility, significant cost saving can be achieved using external cloud services, which inherently provide high availability and reliability.
- **Energy efficient** – The adoption of cloud computing results in more optimised usage of computing resources, which leads to reduced power consumption, contributing to the greening of the global ICT world.
- **Internal IT transformation** – The research and education institution can lower the operational cost for IT maintenance, or, rather, shift the IT focus from system/service administration and

maintenance – “keeping the lights on” – to more valuable activities such as innovation and providing support to core research and education processes.

2.3 Barriers and Challenges

Cloud computing as a relatively new technology also brings new challenges, barriers and risks that need to be identified and considered in the cloud strategy and, if possible, be resolved in the implementation stage in order to exploit the full benefits of cloud services. The barriers and challenges include:

- **Security** – Security is the greatest concern of most organisations in the adoption of cloud services. From the users’ point of view, the areas of greatest 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, and data protection, especially protection of personal data.
  - Identity and access management – Since the cloud services are accessible from anywhere with Internet connectivity and are usually organised in a multi-tenant environment, users are concerned about how identity and access protection is provided and managed by cloud providers.
  - 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 a different legal jurisdiction.
- **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 is in the deployment stack (ascending from IaaS to SaaS) the less control remains with the user over the information management.
- **Integration with in-house systems** – Cloud services in general need to co-exist and integrate with other established IT systems (identity management, networks, monitoring, backup systems, security systems, etc.), which in many cases can be a complex task.
- **Vendor lock-in** – Cloud computing is still faced with the challenge of lack of standardisation and readiness of commercial cloud providers to fully support interoperability. 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.
- **Resistance to new working practices** – Most of the technological changes involved in the adoption of cloud computing have a positive impact. However, some resistance to new ways of working may occur, as it may require new roles, skills, knowledge and responsibilities.
- **Skill sets and resources** – Depending on the cloud solution, e.g. to build or buy cloud services, new skill sets and resources may be required, such as legal and contractual expertise, service management, technical expertise, security management, billing and commercial (if charging to end users).
- **Internal IT transformation** – Aside from the benefit of lowering the cost of IT operation by adopting cloud services, losing in-house IT skills, experience and capacity built up over time could in the long run lead the institution into a position from which it would be very difficult and expensive to revert back.

3 Strategy Synthesis

Based on the comprehensive set of information collected and analysed during strategic analysis, the next stage in developing a cloud strategy is to set strategic goals that reflect the institution's vision – its vision for itself as well as with regard to addressing the user requirements. Different business cases, solutions and implementation scenarios should be investigated to assess whether the goals are realistic, feasible and achievable, and therefore whether the investment is justified. It is an iterative process of strategic thinking, with feedback loops in which some solutions and options can, and most probably will, be discarded, while new ideas and possibilities will appear. By the end, one or just a few preferred solutions should be identified, which represent the best opportunity for cloud deployment with maximum advantages in the most cost-effective way.

3.1 Decision-Making Process

3.1.1 Vision

Setting the goals and making strategic decisions needs to be aligned with the institution's vision and existing strategy, and with other policy documents, such as constitutional acts, bylaws, management and operational principles. The policy environment differs between organisations, but in the context of cloud computing there are a number of initial questions that should be raised in order to drive the strategic thinking, such as:

- What does the institution expect of itself?
- What do others (users, funding bodies, the wider community) expect of the institution?
- What is the institution hoping to accomplish?
- What is required to move forward and achieve the goals?

3.1.2 Users and User Requirements

There are many different answers to the above questions and therefore many possibilities to further develop the cloud strategy. However, the strategy development needs to be based on the output from the previously performed analysis and driven by user requirements and business cases rather than technical challenges. The specific results of this stage of the 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 science" researchers, teachers, students, etc.?
- Which user needs should be addressed – commodity computing or high-performance computing, storage or backup service, collaboration and productivity tools, e-learning, file sharing, etc.?
- Which cloud service model should be chosen – SaaS, PaaS, IaaS or some other?

Again, there is a wide range of possible answer combinations to the above questions and all are focused on which cloud service to provide for the user community.

3.1.3 Provision of Cloud Solution

Once the cloud service has been selected, the next focus of the strategic-thinking process is how to provide the cloud service, with two essential questions helping to define the cloud solution:

- Which cloud deployment model should be implemented or supported – public cloud, private cloud, community cloud or hybrid cloud?
- What will be the role of commercial cloud providers in the cloud service provisioning?

Answering these questions finally leads the institution to the central element of the cloud strategy:

- What will be the role of the institution in the cloud service provisioning?

The rest of this section discusses further the topics that will shape the cloud solution: deployment models and the role of the institution.

3.2 Cloud Deployment Models

When deciding between the different cloud deployment model options, a cloud strategy needs to achieve a balance between the benefits and risks for the institution, taking into account the institution's strengths and the feasibility of implementing the chosen model.

3.2.1 Public Cloud

Public cloud infrastructure is made available to the general public and service provision is owned by the institution selling the cloud services, e.g. a commercial cloud provider. A broad range of public cloud services have already been widely adopted, including by the institutions' user communities (Gmail, Office365, Salesforce, Amazon Web Services (AWS), HP Cloud, Dropbox, etc.). Many of these cloud services are offered free of charge with limited capacity or functionality, which is often enough for individual usage. The users are already familiar with these services, which could be an additional driver for adopting the service at the institutional level with higher quality (extended capacity and functionality).

Public cloud is the easiest deployment model, and relatively fast to implement, but the institution's commitment and involvement are still required, for example in relation to service branding, AAI integration, monitoring, management, user support, etc. For long-term usage, financial stability, with budget reallocation from capex to opex, is essential.

For all the reasons mentioned above, the commercial usage of public cloud services is an increasing trend in the research and education community.

3.2.2 Private Cloud

An institution may wish to consider providing private cloud infrastructure solely to its internal users (researchers, teachers, students). An example of these services is IaaS compute and storage (VMs) for scientific experiments, or SaaS services such as a Moodle virtual learning environment (VLE) service for students. This approach requires significant resources, not only for initial capital investment and

effort to build such a complex service, but to provide long-term operational stability and sustainability. A wide range of technical and management skills and experience is of the highest importance.

3.2.3 Community Cloud

As an extension of internal private cloud, research and education institutions can provide a cloud service to the wider research and education community, by combining their efforts, for example. The platform for community cloud is typically quite similar to private cloud (e.g. OpenStack, VMware vCloud), but providing a community service will add extra requirements and complexity, such as:

- Security requirements to isolate and protect different user environments.
- Need to integrate with users' environment at a network or application level.
- Pricing models with billing and charging functionality.
- Service requirements of users, e.g. service level agreements (SLAs), service management resources.

3.2.4 Hybrid Cloud

The hybrid cloud model could be an extension of both private and community cloud models, 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 private/community cloud can be supplemented by those from a public cloud at particularly busy or peak times. This deployment model is the most complex, and usually comes as an extension on top of the previously built and already complex private or community cloud.

3.3 Institution's Role in Cloud Provisioning

Cloud services are in general highly complex and bespoke, requiring significant organisational resources for development and support activities. While some of the building blocks of such cloud services are well known and often use the core skill sets of IT staff in the research and education community, the additional layers of functionality, such as elasticity, self-service, on-demand usage and billing, bring new challenges. While many organisations have the skill sets to develop cloud services and support them in a production environment, for many others this is not feasible.

No matter which service model is chosen or which deployment model is implemented, only the final service is exposed and visible to the users. In the service provisioning and supplier chain, all the actors – namely, third-party cloud provider (if it is involved), the institution, its staff (technical operations, developers, administrators, managers, etc.) and end users – have their own roles and responsibilities. A simplified view of the relations between these actors is shown in Figure 3.1 below.

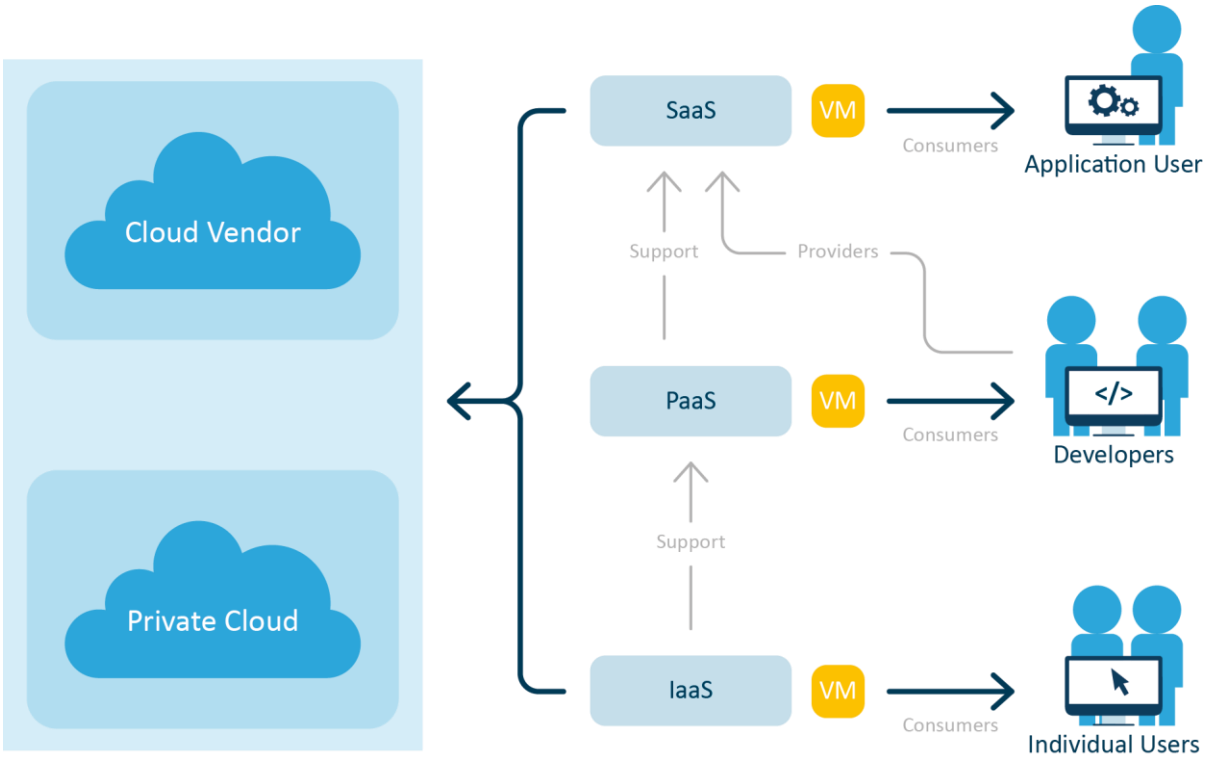

Figure 3.1: Roles and relations of cloud providers, developers and users

The reality is more complex, with many possibilities for research and education institutions to deliver their own cloud services, acting as a provider for their own users, but commercial cloud providers can still play a significant role. Moreover, the options to deliver a cloud service are determined by the roles and responsibilities of these two main actors – the institution itself and a third-party cloud provider – with regard to the following key aspects of 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, compliance, etc.?
- Location – Is the cloud infrastructure located in the organisation's data centre (on-premises) or under the responsibility of the commercial provider (off-premises)?

These three dimensions reflect how the roles and responsibilities are shared between the institution and the third-party cloud provider, as depicted by the cube model shown in Figure 3.2 below.

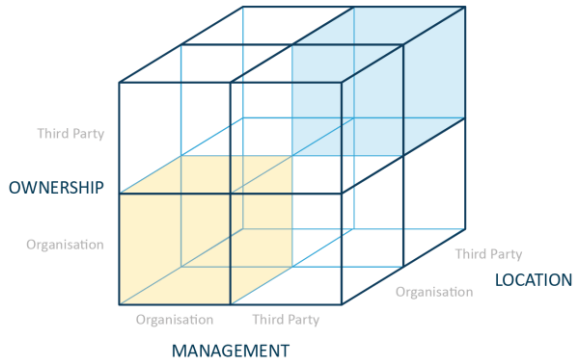

Figure 3.2: Cloud provision options

In the extreme case (top-right back corner), the cloud service is fully outsourced to a third-party provider, who builds and manages the cloud service on its own infrastructure and in its own data centre. Going beyond widely used free but limited usage of public cloud services (mostly SaaS), individual researchers, ongoing projects or institutional departments can easily purchase public cloud services on the global cloud market. Virtual resources can be elastically scaled up to meet demand and released when no longer needed, while the payment is on a usage basis, i.e. pay-as-you-go as users consume resources (storage, network traffic, VM size, IP addresses, etc.). However, it opens up the issues of integration with other institutional services and in-house systems, management of information and processes outsourced to the cloud, legal and contractual challenges, other security issues, etc.

At the other extreme (bottom-left front corner), the cloud service is fully in-house, delivered and provided through a private/community cloud model, developed and managed by the institution itself, running on its own equipment and premises. This approach is appropriate and feasible for some organisations with a large number of end users (NRENs, large universities and institutions, etc.), but requires significant resources (financial, knowledge, skills, time, effort, etc.) and is much higher risk to deliver the service.

A safe approach to consider is to use a commercial cloud provider to deliver a dedicated managed service. In this case the institution can use a commercial cloud provider to provide the resources and expertise to build and operate a cloud service, but with the service still being the institution's. With this approach the cloud provider is effectively providing a managed service. Since a cloud environment is based on multi-layered infrastructure, in this cloud provider model the roles and responsibilities of cloud infrastructure management can be subdivided and shared across the layers of the cloud stack – from the physical hardware virtualisation platform up to the application level. The advantages of this approach are that the institution is in a position to provide a new service without having to invest in building up in-house dedicated technical resources and expertise. This could potentially speed up the process of launching new services by avoiding the time, cost and effort of building specialised teams, and reduces the financial risk. However, 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.

It is worth noting that in all cases the cloud service is considered to be under the institution's ownership and branding.

4 Strategy Implementation

The third stage of developing a cloud strategy focuses on cloud service implementation and usage. For successful cloud adoption with maximum advantages and cost-effectiveness, a detailed cloud service roadmap needs to be defined, with the associated risk management, organisational changes and branding considerations addressed.

4.1 Roadmap Development

To ensure that the cloud strategy is successful, a roadmap is needed to define the major activities and resources required to achieve the strategic goals with acceptable cost, time and effort. The roadmap should consist of the following three major phases:

1. Preparation – Includes activities to prepare the project team and establish the budget and procurement framework, as well as technical activities to specify technical requirements and acceptance criteria, and to design the service with all necessary details to achieve the specification.

2. Implementation – The activities needed to bring the service live, which include conducting the procurement, technical installation, configuration, testing and onboarding, as well as supporting activities, such as project management.

3. Operational – Long-term activities, which include day-to-day service operation, monitoring, reporting, maintenance, support, helpdesk, training, promotion, marketing, etc.

4.2 Risk Management

Implementation of a cloud strategy is likely to be challenging due to the potential risks involved regardless of how well-defined and detailed the plan is. Successful cloud adoption therefore needs to include proper risk management in order to anticipate possible risks at an early stage, analyse their impact, and plan mitigation approaches. The goal is to minimise 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 project plan and budget.

4.3 Organisational Changes

To be able to deliver on its cloud strategy, a research and education institution 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:

- Technical skills in cloud technologies appropriate to the relevant cloud services, e.g. platform-specific skills to test, implement and operate cloud services, storage, billing, etc.
- Security skills to address data protection, identity and access management, compliance with standards and other management and operational security issues.

- Governance, commercial, legal and contractual skills.
- Service management skills to manage an institution's own cloud service or to manage external service providers.

Research and education institutions may have some or all of these competencies in-house, but the organisation structure may need to change to reflect the strategy and impact of cloud services on skill sets and resources.

4.4 Service Branding

The cloud services world is a crowded arena with many service providers competing to get the attention and potential business of institutions. While the research and education community is in general loyal to internal IT infrastructure and services, there is no guarantee that users will choose or even understand the cloud services being offered. The research and education institution will need to compete with strong messages from commercial providers to ensure its users understand its strategy in relation to cloud services and the key benefits. To ensure its messages reach the right audience, it is important to consider:

- The service branding and key messages.
- A communication strategy to deliver the key messages.

These considerations are no different to those facing the commercial providers and the approach is similar. The branding of a cloud service helps users understand its positioning and the unique value that the service brings to the research and education community, e.g. low cost, high performance, ease of use, security, integration with existing in-house systems (AAI, monitoring), etc.

5 Conclusion

Cloud services present research and education institutions with many opportunities and benefits but also with significant challenges and risks. A methodology to define a cloud strategy, as outlined in this document, is essential to ensure that the right services are identified, designed and delivered using the approach that best fits the users' and institution's requirements and capabilities, consistent with the institution's overall strategy and vision.

References

[CloudImplications] D. McDonald, A. MacDonald and C. 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

[CloudStdsRoadmap] M. Hogan, F. Liu, A. Sokol and J. Tong, *NIST Cloud Computing Standards Roadmap*, Special Publication 500-291, Version 2, July 2013 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf

[CloudToolkit] N. Convery, *Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud*, Department of Information Studies, Aberystwyth University, August, 2010 https://www.aber.ac.uk/en/dis/latest-news/news-archive/title-99448-en.html

[DigitalAgenda] *The Digital Agenda for Europe: Driving European growth digitally – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2012) 784 final 18.12.2012 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1582560442205&uri=CELEX:52012DC0784

[e-IRG_CloudComputing] e-Infrastructure Reflection Group (e-IRG), *Cloud Computing for research and science: a holistic overview, policy, and recommendations*, 30 October, 2012 http://e-irg.eu/documents/10920/238968/e-irg_cloud_computing_paper_v.final.pdf

[GÉANT] https://www.geant.org/About

[GN_CloudStrategyGuide] S. Gajin, R. Hackett, J. Pagaime, D. Cresti, F. Galeazzi, M. Grammatikou, E. Mirzamany, S. Leinen, *NREN Cloud Strategy Guide* https://clouds.geant.org/wp-content/uploads/2016/08/NREN-Cloud-Strategy-Guide-final.pdf

Glossary

AAI	Authentication and Authorisation Infrastructure
AWS	Amazon Web Services
CRM	Customer Relationship Management
e-IRG	e-Infrastructure Reflection Group
HP	Hewlett-Packard
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
NIST	National Institute of Standards and Technology

NREN	National Research and Education Network
PaaS	Platform as a Service
R&E	Research and Education
SaaS	Software as a Service
SLA	Service Level Agreement
VLE	Virtual Learning Environment
VM	Virtual Machine