Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jörg Sambleben
Erschienen im Magdeburger Institut für Sicherheitsforschung

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

From Misconceptions to Failure

Security and Privacy in US Cloud Computing FedRAMP Program

Mikhail Utin, PhD

This Articles considers practical implementations of »Cloud Computing« (CC) and associated services (CCS) in the US FedRAMP program, which is expected to convert all the government IT services into »cloud« based ones. We conducted the research on how this concept helps to secure information in IT infrastructures. In particular, we were interested to see how it provides security in such a large-scale implementation as the US government FedRAMP program.

The following papers were analysed: NIST SP-800-53 R4, NIST SP-800-37 R1, NIST SP-800-144, NIST SP-800-145, NIST SP-800-146 and FedRAMP.

Citation: Utin, M. (2015). From Misconceptions to Failure: Security and Privacy in US Cloud Computing FedRAMP Program. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 628–660. Retrieved October 25, 2015, from http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Version 2015/12/03 10:46

1 Introduction

In our previous analysis of »cloud computing (CC)« (M. A. Utin and D. Utin 2012a) at DeepSec 2012 and OWASP AppSec DC 2012 (M. A. Utin and D. Utin 2012b) we have concluded that CC is a generally misleading, marketing-driven concept, born out of the need to utilize hosting services which became overly-abundant post Internet Bubble. Well-known CC models are useless, and in the case of the so called »community cloud« model it amounts to little more than legal nonsense. To analyse »cloud« security requires to consider deployment, service and security models. Altogether a structure of enormous complexity, consisting of multiple overlaying models and implementation options, and thus useless for any security research and analysis.

In the case of the implementation of high level complex regulations like the EU General Data Protection Regulation (GDPR) (European Parliament 2012), CC is not only useless, but by being misleading, it creates a dead-end situation where it is not possible to identify how exactly privacy will be protected in an Internet-based distributed computing environment.

However, regardless of numerous concerns regarding CC Services (CCS) expressed by information security professionals the US government developed the FedRAMP program (US General Services Administration 2012) funding the moving of federal information systems into a »cloud«, based on a »»Cloud First«« policy. Our research shows that all »cloud« misconceptions have successfully made it into NIST (National Institute of Standards) and FedRAMP documents.

What should we expect from such a large scale experiment as the FedRAMP program?

What will be the result of the »cloudization« (our term for converting local IT system into »cloud«-based systems) of US federal information?

Will it be a waste of taxpayers' money while a few people achieve some political gain, capitalizing on the public inability to distinguish between technological opportunities and technological opportunism?

Or is this the next technological step toward moving and processing data from and to wherever we want?

To understand what happened so far and to prevent the world yet from another failure sold as an achievement, we need to dig deep into the research of fundamental US government documents related to CC and CCS (Badger et al. 2012; Jansen and Grance 2011; Mell and Grance 2011), risk management (Ross and Johnson; 2010), security controls for federal information systems (Ross 2013) and FedRAMP itself (US General Services Administration 2012, 2014a; Virka 2013) to draw our conclusion based on thorough analysis of these documents and known CCS implementations.

In particular we will be looking for:

- Any proof that cloud computing provides a better explanation and a better model of hosting services;
- Advising on CC security implementation issues;
- Advising on CC security risks;
- Cloud specific security and privacy controls and implementation of security controls and privacy protection;
- Advising and proof of economic advantage of CCS;
- Advising on cloud specific legal issues;
- Results of published official auditing of existing CCS

While we were in full-steam research, we received shocking news:

In July 2013 NASA's Office of Inspector General published an audit report: »NASA's Progress on Adopting cloud-computing Technologies« (US General Services Administration 2014b).

Translating the audits politically correct language into normal technical terms and taking into consideration that this report includes about 100 web sites never tested for security before and many of them having no security at all we can say that it's a complete failure of the agency to address security issues while transferring a part of its IT services to CCS.

Financial aspects were unfortunately not one of the objectives of the audit, but the following logical conclusion is obvious: Security Failure will affect the expected reduction of costs.

If any of such saving could happen at all.

To understand why such failures have happened and what we should expect from the further implementation of FedRAMP, we need to start our analysis right at the entry point of »cloud computing«.

Our analysis of various government documents will help to investigate the entire path of the program from the start right up to early 2014.

Then we may answer the most important question: Whether »cloud computing« can be used at all to save governments money by transferring IT services to a »cloud« and yet keeping security up to the required compliance level - or not.

The rule »garbage in – garbage out« has been proven on numerous occasions. We are going to research whether it is applicable to »CCS – FedRAMP« and if and why the program is set to fail.

2 Where does »cloud computing« come from?

The history of CC goes back to the Internet Bubble, which required a lot of data centers hosting a rapidly growing number of web sites. After the Bubble had burst, many data centers became useless. Some sources state that at the low point only 10% of their power was used. In 2006 Amazon.com came up with the idea of hosting applications in the same way as web hosting - there is a consensus that Amazon Web Services (AWS) is the predecessor of CC services. How »hosting« service became »cloud« is the matter of our research below.

2.1 Where does »cloud« come from?

The past of »cloud computing« itself is cloudy, but so much's for sure: Amazon.com was not talking »cloud« when it started AWS. Neither did Google when it started its Academia Cluster computing Initiative (ACCI) (Bisciglia 2007) in 2007. ACCI was interested in Distributed Parallel Processing (DPP) and nothing else.

Alfred Spector, VP of Google research says in his post (Spector 2011) »Academic Successes in Cluster computing« in December 2011: »Access to massive computing resources is foundational to Research and Development. Fifteen awardees of the National Science Foundation (NSF) Cluster Exploratory Service program have been applying large scale computational resources donated by Google and IBM.«

Thus, neither Google nor the NSF, as leading US government organization funding research, ever considered »cloud« projects - contrary to common belief or to what one can find, for instance, on Wikipedia:

In it's article about »cloud computing« referring to ACCI it says »In October 2007, the Academic cloud computing Initiative (ACCI) was announced«. That is completely wrong!

ACCI means Academic Cluster computing Initiative: the first C stands for »Cluster« not »cloud«. Needless to say that »cloud« and »cluster« have noting in common in terms of computer science.

Such a replacement is a sort of violation of Google.com's intellectual property rights on ACCI.

But then where did »cloud« come from? We have traced it to IBM circles and associates. Cloud associated site cloudBook.net explains: »IBM / Google Academic cloud computing Initiative (ACCI) - The IBM/Google initiative aims to provide computer science students with a complete suite of open source based development tools so they can gain the advanced programming skills necessary to innovate and address the challenges of the cloud computing model« (cloudbook 2013).

cloudBook.net changes the purpose of Google's ACCI project from research and the utilization of clusters to »the challenges of the cloud computing model«, thus making the word »cloud« a legitimate term and transforming the ACCI cluster project into a »cloud« project.

IBM does not have an »ACCI« equals »Academic cloud computing Initiative« statement on its official sites. However, it is very likely that the company utilized its satellites' finding and then started to use the newly invented term for pure marketing reasons, to sell its numerous »after Bubble« resources and services.

2.2 Terminology. And is there such a thing as »cloud« computing?

The term »cloud« never appeared in computing Science and never was associated with it. Yet another incorrect statement from an Wikipedia article (Wikipedia 2014c) states that »... In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time.«

As already mentioned above and in reference to the work of Bisciglia (2007) and Spector (2011), academia and science used the well-known terms »cluster« and »Distributed Parallel Processing« for distributed computing projects. Computer science did not and does not use the word »cloud« as a synonym for distributed processing - simply because the purpose of »cloud« was no computing at all.

We know Analog computing, which was the beginning of computing. We know Digital, Multiprocessor, Mainframe, Cluster and DPP: Each identifies which computational method is being used.

Yes, DPP can run the same program over the Internet to split a calculation between processors to speed it up. However, in such examples of CCS as Amazon's AWS, and others as well, we do not see multiple instances of the same program working on the same task as in DPP.

Instead, each instance of the »cloud« (host, application, or service) serves its own purpose. Instances are not expected to split the same data set between them to crunch numbers and then to combine parts in a resulting data set. Each »cloud« process works with its own data set independently and produces its own result.

The »cloud« term and depicting image has been in use for years, first in communications later to represent networking basically as a communication environment.

It has been used to describe a mash of communication lines, communication equipment and protocols with the pure purpose of connecting two communicating piers.

The purpose of »cloud« was and is to transmit information, not to do computing. A typical example is a web service, where information is kept on the server, transmitted to a browser, and gets delivered to a user after a certain interpretation. We will consider the nature of CC in detail in our next paragraph.

2.3 Conclusion

The term »cloud« appeared more likely within IBM affiliated circles. It started by replacing »Cluster« in the Google originated program name »Academic Cluster Computing Initiative (ACCI)« by »cloud«.

The incorrect name of the ACCI program still exists in Wikipedia articles and on IBM affiliated web sites.

But »cloud« came from communications, not computer science. The nature of the »cloud« is communication, to deliver information utilizing hosting services. There is no such computing.

3 Models and CC concept

As we already stated above: »cloud« is a communicational term, while »computing« belongs to computer science. Connecting these two words was a brilliant idea to introduce the »new« service of »cloud computing« as a new computing concept - nothing but a pure marketing trick, the invention of a a new brand name to use instead of the old term »hosting«.

To claim it a »new computing concept« CC required some sort of a science behind it. It needed a model as a standard science attribute. That is why the Deployment and the Services model (Wikipedia 2014a), have been developed. However, the question whether these models have any value remains and should be answered.

We need to admit that, so far, the exact author of the »cloud computing« term and the models is yet unknown - so the prize for a »trick that changed the world« still remains unrewarded.

Before discussing »cloud« models, we need to answer in general why we need and use models:

A model is a structured representation of something of »the outside world« that people can consciously use as guidance. If a model is incorrect, then a person can be involved in useless or dangerous activity.

Thus models have to represent the outside world adequately so that they can be utilized for planning useful activity.

Now we are ready to discuss CC fundamentals. There are two models, which are used to describe CCS implementation – the Deployment Model and the Service Model. The first relates to the networking infrastructure, and the second to services within such an infrastructure.

Following our statement above, we need to examine if these models are adequate and useful, and, if so, to which extent. We will begin with the Service Model to clarify what exactly CC does, and if there is a difference to what we had in the era »before cloud«.

3.1 CC Service Models

There are four models - Network as a Service (NaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), – whose definition and/or description can be found in the NIST publications (Badger et al. 2012; Jansen and Grance 2011; Mell and Grance 2011), or in Wikipedias »cloud computing« article (Wikipedia 2014a). The NaaS model (Wikipedia 2014a) is relatively new, and did not exist during the writing of the NIST documents (Badger et al. 2012; Jansen and Grance 2011; Mell and Grance 2011). The referenced sources contain numerous details, which we will skip to simplify our task of digging up the essence of the services in question.

3.1.1 Network as a Service (NaaS)

The related article on Wikipedia (Wikipedia 2014a) does not give a definition of this model, but has some sort of vague description what it does. The most useful part of it is »NaaS concept materialization also includes the provision of a virtual network service by the owners of the networks infrastructure to a third party«.

We translate that to: »NaaS is a virtual network application which is provided to CCS customers«, or shortly to »Hosting of a virtual network«. Because that's what NaaS is – nothing more and nothing less but hosting.

3.1.2 Infrastructure as a Service (IaaS)

Quote from NIST (Mell and Grance 2011): ». . . providers offer computers, as physical or more often as virtual machines, and other resources«. Virtual network components have been originally placed in Infrastructure as a service, and quite logically so, because there is no difference between physical and virtual components when they are accessed and controlled remotely. The appearance of the virtual NaaS model is likely to be a marketing attempt to introduce »new« services. Finally, what is IaaS? Hosting of a customer network on vendor premises, either virtual or physical. Again – nothing more and nothing less but hosting.

3.1.3 Platform as a Service (PaaS)

Quote Wikipedia (Wikipedia 2014a): »cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform«. In brief, a vendor provides remote application development environment where the customer can host the development process. Nevertheless, it is an application development environment hosting service. Again. Nothing more and . . . .

3.1.4 Software as a service (SaaS)

It is the applications' hosting environment, where a customer can run various applications – office software, email, games, etc. The difference to PaaS is that SaaS does not provide access to OS and the development environment. However, it is the same kind of hosting service, which has been introduced as AWS by Amazon.com in 2006.

Considering that the CC services in question are simply hosting services and have a dynamic nature (service can move between infrastructure nodes), we can call cloud computing a Dynamic Hosting Service utilizing the terminology (Dynamic and Hosting Service), which has been used a while before the CC initiative. We would like to note that the CC terminology does not point to the dynamic nature of its services.

Table 1 represents an interpretation of Service Models in simple and understandable hosting service terms.

We used the old terminology of »Hosting Service« to name and thus describe the collection of CC Services. In the table above we show that there is no need to invent and use a special »CC Service Model«, because all processes can be easy explained by using terms of the traditional Hosting Service vocabulary with modifications in each particular case.

3.2 CC infrastructure Deployment Models (DMs) and terminology

We have discussed the Service Models and it helped us to confirm that CC is a service, actually a pure Hosting Service, allowing to move information freely across organizational borders.

The idea behind the CC Deployment Model is to explain how networking infrastructure is installed, in general it's about vendor resources.

The first question is why a customer needs to know about the whereabouts of the CC Service he's using.

For instance, when we get an Internet connection from an ISP, do we really care where the ISP is located or about its infrastructure?

The second question - one we've already answered concerning Service Models – are Deployment Models adequate and useful?

Since 1985, when AppleTalk has been introduced as the first Local Area Network (LAN), we utilized just a few terms describing the evolution of networking.

There are two fundamental terms: LAN and WAN (Wide Area Network (Wikipedia 2014c)) with a few technological sub-types like WLAN (Wireless LAN) and SAN (Storage Area Network).

When somebody says to us »LAN« or »Wireless LAN«, we definitely know what it means – local, i.e. inside one's jurisdiction, a collection of computers means LAN, peripheral equipment and networking means, either wired or wireless.

WAN is a broader term, and can refer to two subtypes: Enterprise WAN and Personal WAN. The latter is a connection from an home computer or LAN to an Internet service provider.

The following is the description of each Deployment Model from NIST 800-144 (Jansen and Grance 2011). So far there are four of them:

(1) »public cloud«

Quote: »...It is owned and operated by a cloud provider delivering cloud service to customers«. Basically, »owned and operated by a provider« and »delivering … service to customers« implies a WAN providing Hosting Service. In the context of the model in question, we can say that public cloud is Personal WAN.

However, do we really need a new concept and a model such as the public cloud to explain what we know since the 1990s as Personal WAN and a connection to an Internet service provider?

(2) »private cloud«

Quote: »… is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it.«

If a private cloud comprises the customer's equipment and is managed by the organization, it is either LAN or WAN, depending on whether it is geographically distributed or not.

If the organization's LAN or WAN is operated by an external entity, this is called »outsourcing«. So, again, we can easily explain the new »private cloud« model in old and easily understandable terms: LAN, WAN, or Outsourced LAN or WAN. Such well-established terms are much easier to comprehend and use than the new »private cloud« , which requires additional explanation of what it is exactly in LAN/WAN and outsourcing terms.

Using old terminology a »private cloud« is an »organizational LAN, which is hosted by a service provider«. In CC language we need to say a »private cloud, which consists of an organizational LAN, and which is hosted by a service provider«. As we see, we used 9 words in the first case and 16 in the second, and »private cloud« is an useless addition to the networking based explanation.

Thus, the private cloud is a confusing and useless model.

(3) »community cloud«

Quote: »community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them«

In a legal context this definition is wrong. There is no such legal entity as a »community«, thus its legal representation outside of such a community is not possible, and services cannot be provided.

Here is an example illustrating that. Alice and Bob (either individuals or organizations) have mutual interests and regulatory considerations. They both want to get a new sort of Internet connection.

Bob calls to an ISP on his and Alice's behalf and talks to a representative:

- Bob: We would like to get new Super Fiber Optic connection!

NaaS	Network as a service	Dynamic Virtual Network hosting
IaaS	Infrastructure as a Service	Dynamic Network hosting
PaaS	Platform as a Service	Dynamic Development hosting
SaaS	Software as a Service	Dynamic Application hosting

Table 1: Relationship between CC Service Models and Hosting Services

- Sales: No problem! I will be glad to do that! Who are you?
- Bob: We are Alice and Bob and we are a customer community as well.
- Sales: Thank you Alice and Bob! But what do you mean by »community«? Are you a company or an organization?
- Bob: No, we are a community, we are separate persons (or businesses), but have mutual interests and regulatory considerations!
- Sales: (after a minute of silence) I do not understand. Do you have a legal agreement of incorporation, or anything else representing you both as a legal entity? We can make a contract and a Service Level Agreement (SLA) only with a legal entity like an individual or a corporation.
- Bob: No, we do not have any legal agreement, because we are, say, an informal community.
- Sales: I do not know anything about communities, but you have to have a legal representation of yourselves in a form of a legal document according to local and federal regulations. I do not have a contact and SLA for a »community«. Sorry …
- Bob: Really? I've red in numerous documents that we can be a »community cloud« receiving CC Services …
- Sales: We do not sell a »cloud«, we sell real ISP services, which require separate agreements with individuals or a businesses. So you, Bob, and Alice, each will have a contract and SLA.

Thus, Bob does not have the option to get an Internet connection as a »community«. If he insists on it he would need to go to court to sue the ISP, and fight a legal battle for the next several years without any Internet connection.

Needless to say that even a CC Services company will have separate contracts and SLAs with each individual or company, simply ignoring the »community model«.

Two pictures that NIST SP-800-146 provides (Figure 5 and Figure 6, pp. 4-10 – 4-12 Badger et al. 2012) do not help to identify legal relationships either.

If a »community« comprises organizations connected to the cloud on a one-to-one basis (i.e. each having a separate agreement with a provider) it is a »public cloud«, as we just discussed above, i.e. a WAN/Hosting Service.

If NIST is trying to explain that a »community« has only one agreement with a provider, then this is legally inconsistent as we see from our considerations.

A »community« is not a legal entity and cannot sign an agreement, unless organizations within such a »community« form a new legal entity.

In this case, it is a one-to-one relationship again, and the »community cloud« converts into a »public cloud«, which is a WAN/Hosting Service.

So far, there is no legal practice of service agreements between a vaguely defined »community« and a service provider.

Really discouraging is that NIST, which discusses SLA and the importance of agreements and contracts with CCS providers throughout its documents (Badger et al. 2012; Jansen and Grance 2011; Mell and Grance 2011), has not discovered the legal absurdity of the »community cloud« model.

(4) »Hybrid cloud«

Quote: »… more complex than the other deployment models, since it involves a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them. « As far as services are concerned, this model is a combination of WAN (private cloud), WAN/hosting service (public cloud), and the »community«, which, as we discussed above, does not legally exist.

3.3 Conclusion

The goal of our examination of CCS models was to identify if there is any value in these models. After our analysis, which we hope was thorough but not excessive, we can say that:

There was no need to invent and use a »CC Service Model«; all processes can be more easily explained using traditional Hosting Service terms. This model is confusing, not adequate and useless.

So named »Deployment Models« are useless for customers to explain the infrastructure used to implement CCS. The old terminology of LAN/WAN and Hosting Service explains it much better, without confusing service providers and users. The »community cloud« is legal nonsense; the »Hybrid Model« is either legal nonsense as well or simply WAN-based infrastructure.

NIST, which discusses SLA and the importance of agreements and contracts with CCS providers throughout its documents (Badger et al. 2012; Jansen and Grance 2011; Mell and Grance 2011), has not discovered the legal absurdity of the »community cloud« model.

The Table 2 below summarizes our examination of »Deployment Models«. There is no computer science behind »cloud computing« itself and neither its terminology nor the invention of a »Service Model« and »Deployment Model« did help making it »scientific«. The essence of cloud computing is the marketing and sale of old Hosting Services, which did not change since the introduction of AWS in 2006.

There is no cloud, there is only hosting - whether it is the hosting of virtual networks or office applications.

4 US Government NIST SP 800 documents identifying information security for CCS

According to our plan, after the clarification and identification of the essence of CCS, we proceed to the analysis of the main US government documents related to CCS security.

The US government requires the implementation of information security according to government standards developed by the National Institute of Standards (NIST).

There is the Information Security Special publication series SP 800: All its standards are mandatory for implementing in the federal information system, and others may follow NIST's recommendations as »best practice«.

Currently there are 151 documents available on the NIST web site, and some of them have additional or draft versions as well (see http://csrc.nist.gov/publications/PubsSPs.html).

There are five NIST documents, which we should consider and analyze to understand the US governments position on cloud computing security.

The first three were developed especially for CC/CCS:

- NIST SP-800-145 - The NIST Definition of cloud computing, September, 2011 (current version) (Mell and Grance 2011)
- NIST SP-800-146 - cloud computing Synopsis and Recommendations, May, 2012 (current ver.sion) (Badger et al. 2012)
- NIST SP-800-144 - Guidelines on Security and Privacy in public cloud computing, December, 2011 (current version) (Jansen and Grance 2011)
- The next document - NIST SP-800-37 R1 - Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010 (Ross and Johnson; 2010) - should help us to understand the risks associated with the implementation of CCS.
- And the final document - NIST SP-800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 - identifies security controls in government systems including CC/CCS.

4.1 NIST SP-800-145 - The NIST Definition of cloud computing, September 2011 (current version)

This document is very short, 7 pages in total, including only 2 pages of technical material (Mell and Grance 2011)

4.1.1 The document analysis

The purpose of the document is identified as (quote): ... »cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a mean for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what cloud computing is to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.«

It contains definitions of Service and Deployment Models and essential characteristics. We have already analyzed both models above - the characteristics are irrelevant to our research, so we skip them.

4.1.2 The document analysis conclusion

This very short document provides what is well-known from other sources, and actually does not live up to its advertised purpose. As stated above (quote): » The NIST definition characterizes important aspects of cloud computing and is intended to serve as a mean for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. «.

In its two pages of technical text we did not find any baseline or any explanation »... how to best use cloud computing«.

In short, this document is almost useless.

4.2 NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version)

This document is in total 81 pages long, including 74 pages of technical text and 5 appendixes. This, as a more general document on CCS matters, should have appeared before NIST SP-800-144, which explains security control implementation. However, the publishing dates are in opposite order (Badger et al. 2012).

CC DMs	What is it concerning networking and services?
Public Cloud	WAN infrastructure for Hosting Service
Private Cloud	LAN, or WAN, or Outsourced LAN or WAN
Community Cloud	Legal Nonsense, or Public Cloud–WAN infrastructure for Hosting Service
Hybrid Cloud	Combined WAN, or WAN/Hosting Service, or Legal Nonsense

Table 2: Interpretation of CC Deployment Model in well-known components and services

4.2.1 The document analysis

The purpose and the scope of the document are (quote):« … to explain the cloud computing technology area in plain terms, and to provide recommendations for information technology decision makers.

cloud computing is a developing area and its ultimate strengths and weakness are not yet fully researched, documented and tested. This document gives recommendations on how and when cloud computing is an appropriate tool, and indicates the limits of current knowledge and areas for future analysis.«

In the very beginning of this conceptual document NIST cautiously explains that CC (quote) »… strengths and weakness are not yet fully researched, documented and tested.« Nevertheless, NIST is going to provide »… recommendations on how and when cloud computing is an appropriate tool … « We will follow the document structure, analyze NIST's recommendations and comment on it.

Executive Summary

The most important found is that the document in question does not follow the current IT mainstream opinion of the economical advantage of CCS by default.

Quote SP-800-146: »Economical consideration: … Whether or not cloud computing reduces overall costs for an organization depends on a careful analysis of all the costs of operation, compliance, and security, including costs to migrate to and, if necessary, migrate from a cloud.« The problem here is »careful analysis of all the costs«.

If a transition to CCS is expected to take several years, like, for instance, FedRAMP plans, then how to estimate a future cost reduction, which will happen several years later and depends on factors and costs yet unknown?

And, in particular, how to estimate the cost of rolling back from CCS when rolling in is yet to be implemented?

Here we can refer to the personal consulting experience of the author. One of the major US health insurance companies in the state of Rhode Island (US) was looking for a person helping them to gain back some control on its completely outsourced IT. To cut down costs the insurance company had outsourced its entire IT staff, except for four IT executives.

After two years it dawned on them that they had no idea what the outsourced IT was doing, even on management level. They wanted to regain a certain level of control and the problem was that they had no idea how to do that. This is very typical for any outsourcing, including CCS. If it is done, its much harder to undo, if possible at all. And the cost of rolling back is not possible to estimate.

This honest NIST statement basically negates the possibility to define the economical advantage of moving in CCS while it is in its design phase because future costs cannot be evaluated.

Cloud Computing Definition (Section 2)

There is nothing new in this chapter. It repeats NIST SP-800-145, which we considered above.

Typical Commercial Terms of Service (Section 3)

This chapter is NIST consideration and advising on the legal part of CCS and what a customer should know and do.

Our general impression is that this section is written keeping in mind old style hosting, not a »cloud«. We also do not like that the problems and following recommendations are considered before the general introduction of cloud environments in Section 4. It would be far more logical to introduce the environments before discussing their problems.

We quote some of NIST recommendations and give our comments:

(1) Terms of Services

Quote: »A consumer 's terms of service for a cloud are determined by a legally binding agreement between the two parties often contained in two parts: (1) a service agreement, and (2) a Service Level Agreement (SLA).«

Discussing two general types of binding agreements NIST considers only two parties – a customer and a provider.

What if CC services are provided by multiple vendors? Or does NIST expect always only one legal entity in a cloud? Then this would be no »cloud« at all.

Multiple CCS vendors within a cloud create a completely different legal situation as we have considered in our talk about private Information Protection in cloud computing (M. A. Utin and D. Utin 2012b). Multiple legal entities mean multiple agreements, delegations of trust, certifications, etc. NIST is not up to discuss that yet.

(2) Data Preservation

NIST presents us with a very general consideration of how usually data is kept by a vendor. However, again NIST pictures a »hosting« vendor, not a »cloud« of vendors.

There is no consideration about how a »cloud« of multiple vendors preserves data, what technical and legal mechanisms are at work, and what will happen in a case of a data loss.

Data is expected to circulate in a cloud, sometimes across national borders, and thus we have international legal issues.

What are the legal means required for a customer 's survival when data is corrupted or lost? Imagine a small company, which completely outsources its financial and accounting information to a cloud - and the information gets lost.

Legal liability is one of the most important parts of any legal agreement, and it is completely missing from this NIST document. The reason for this is that NIST is an US government organization, and the government lacks practice in suing private entities for government's data loss. Currently known government cases are about recovering monetary damages (like overbilling) from a private entity or penalizing someone for the loss of legally protected data like personal information. However, if the government outsources its (actually – public) data and the data gets lost is another matter. NIST has yet to understand that such gaps of legal recovery from business losses in a cloud need to be addressed.

(3) Force majeure events

Quote: »Providers generally disclaim responsibility for events outside their realistic control. Examples include power failures, natural disasters… «.

Again, NIST has a small »hosting« local data center in mind, not a »cloud«. And again, there is no advising how to legally deal with such a situation. Things like power failures, and even natural disasters should not affect a well planned and working data center, not to mention a »cloud«. Providers should guarantee a very high degree of service reliability even in a case of disaster. And, of course, contracts should contain legal liabilities as we proposed above. Otherwise, what is the difference between outsourcing to a provider with one plain server and no redundancy and a »cloud« of monstrous facilities almost capable to withstand a nuclear strike?

By the way, customers pay for such physical reliability, so why legal liability is completely missing from NISTs consideration?

(4) Security

Quote: »Providers generally assert that they are not responsible for the impacts of security breaches or for security in general …Generally, service agreements are explicit about placing security risks on consumers. In some cases, providers promise to use best efforts to protect consumer data, but all of the providers surveyed disclaim security responsibility for data breach.«

So, why do we need a »cloud« when nothing is guaranteed? NIST tells us how things are according to the wishful thinking of CCS providers. However, customers need advising on how CC Security should be legally guaranteed, no storytelling. In particular, when it comes from such a highly regarded resource as NIST.

In its own case such general considerations and the absence of real advising led the US government to FedRAMP misconceptions and the following NASA »cloudization« security problems (US General Services Administration 2014b).

(5) Recommendations

Here NIST gives very short and general advise (quote):

»… consumers may wish to formulate and negotiate remedies that are commensurate with damage that might be sustained.«

We think that customers not only wish but have to put certain legal means in the SLA and/or their contract to re-mediate the situations we considered above, namely at least data losses, force majeure events, and security breaches.

Quote: »Compliance. Consumers should carefully assess whether the service agreement specifies compliance with appropriate laws and regulations governing consumer data ».

However, if the provider specifies compliance, how could the customer be sure that it has been really achieved?

We have seen providers saying »We are HIPAA compliant«, and then failing to deliver any internal security documents confirming their claim. Needless to say that document statements are not enough either.

NIST, what would you advice us to do in such cases?

General Cloud Environments (Section 4)

In this chapter NIST considers deployment models and (quote) »…describes general implications for different deployment options«.

Basically, this means the consideration of a model and its issues. However, the material is not well organized in our opinion, and contains additional terminology such as »scopes« (we would prefer to call them issues), »scope modifiers« and »statements«, as well as others.

Initially provided general scopes are:

(1) Network dependency

(2) Consumers still need IT skills

(3) Workload locations are dynamically assigned and thus hidden from clients

(4) Risks from multi-tenancy

(5) Data import/export and performance limitations – And some additional scopes.

In our analysis we will skip three deployment models: the »On-Site community cloud«, »Outsourced community cloud« and the »Hybrid cloud«.

As we discussed above, any model related to a so called »community« is legal nonsense, thus we should not waste our readers' time considering matters of nonsense.

(1) Network dependency – for three models - On-Site private cloud, Outsourced private cloud and public cloud - NIST discusses what is well-known about LAN and WAN: Internal vs external services, availability and the quality of communications connections. There is nothing new in that.

(2) Consumers still need IT skills – Traditional IT skills are required during migration (On-Site private cloud) and very likely will be needed in the cloud. And new IT skills will be needed for a cloud. Pretty obvious considerations.

(3) Workload locations are dynamically assigned and thus hidden from clients – On On-Site private cloud NIST just tells us what we already know about the migration of workload between computing resources locally, the virtualization, and geographically – WAN. Outsourced private cloud and public cloud are explained very similar, just using some different words.

(4) Risks from multi-tenancy – This has always has been a problem of sharing resources. A mismanagement of access leads to an information compromise, and this is true for any type of sharing (in our case On-site private cloud, Outsourced private cloud and public cloud).There is nothing new in that.

(5) Data import/export and performance limitations – basically NIST says that resources may limit performance, but can be added to the »cloud«, i.e. in LAN or WAN (On-Site private cloud). According to NIST the same is applicable to communications in an Outsourced private cloud. The public cloud is missing from this »scope« considerations for unknown reason.

Next NIST moves to various additional scopes mixing and matching various scopes:

(6) Potentially strong security from external threats – NIST talks about the On-Site and Outsourced private cloud but not about the public cloud. Is it because public cloud is too secure to be discussed or completely insecure?

(7) Significant-to-high up-front costs migrating into the cloud - That's what NIST in general expects, decreasing such costs to modest-to-significant for an Outsourced private cloud and to low for the public cloud. The latter assumption remains unexplained while the expectation concerning the significant-to high costs for an On-Site private cloud is based on »cloud software« deployment costs.

But why is it costly? Technically speaking »cloud software« is a virtualization, almost a standard IT solution for most mid-and large size organizations and thus it may already exist as in On-Site private.

(8) Limited resources (available from customer pool) are identified as such for On-Site private cloud. However, this it is more a »cloud« theory than a virtual reality, because in any modern network there are spare resources and virtual hosts available.

(9) Restrictive default service level agreement – the last item on NIST's list and it's about private cloud only. NIST consideration is known from the above – providers restrict customers. However, it would be better providing good advice than plainly stating common but incorrect practice.

Software-as-a-Service (SaaS) Environments (Section 5)

The purpose of this section is »... to describe the architecture and basic operations of SaaS ... whether a SaaS cloud offering can satisfy particular reliability, compliance, or security requirements, and also for readers who want to understand operational mechanisms.«

In this preamble NIST explains that »... different definitions of SaaS are possible, a simple and usable definition has already been formulated: Software deployed as a hosting service and accessed over the internet«.

That is what we advocated in our presentations and articles – SaaS, as other »cloud« models are useless and the old term »hosting« can always be used instead.

NIST then considers »... important characteristics of SaaS offering«:

(1) Abstract interaction dynamics - NIST provides us with some sort of abstract and a model describing what is actually known about resources, applications and about utilizing them; it is helpful but not really important.

(2) Software stack and provider/consumer scopes - Very similar has been considered before: What cloud Provider and cloud Customer control in a mutually used »software stack« of Application, Middleware, Operating System and Hardware layers. Simply put, customer controls only the Application level. There are some nuances, but they're not really important.

(3) Benefits - Which are:

(3.1) Very modest software tool footprint – mostly because the web browser is used as an universal client.

(3.2) Efficient use of software licenses – per connection rather than for each application.

(3.3) Centralized management and data: expected to improve security by providing it in the »cloud«.

(3.4) Platform responsibilities are managed by the provider -infrastructure (or »platform« here) management is the responsibility of the provider.

(3.5) Savings in up-front costs - utilizing applications without equipment acquisition.

However, in our imperfect world, these »cloud« advantages can be lost due to providers' mismanagement or security exploits. NIST briefly considers various issues as below.

(4) Issues and concerns:

(4.1) Browser based risk and risk remediation – Microsoft Internet Explorer, by various sources (all versions), still owns approximately 50% of the worlds browser market. At the same time, it is traditionally the most vulnerable and exploitable one. These two factors create a significant risk of exploitation including the compromise of the entire cloud.

(4.2) Network dependence - bad or failing connection can be a real problem. How much would one hour of downtime cost your business?

(4.3) Lack of portability between SaaS clouds - all »clouds« are actually proprietary hosting services (i.e. data centers), and there is almost no way of moving back from or switching between providers.

Moreover, providers do not really want either customers switching providers or applications transferred between »clouds«.

(4.4) Isolation vs. efficiency (security vs. cost tradeoffs) – it is usually unknown whether each customer has his own copy of a cloud application or if the application is shared and completely out of the customer's control.

That creates additional risks, as, for instance, in a case of one shared application and a browser attack, when all customers may be compromised.

(5) Candidate application classes:

NIST considers various kinds of applications utilizing SaaS. We do not understand the purpose of listing obvious descriptions. Applications like real-time control (robotics of flight control), bulk consumer data (medical devices) and critical (may cause loss of life or significant property loss) software are out of CCS scope indeed. Nevertheless, it is known that multiple hospitals and companies utilize medical records' SaaS, and do not consider that corruption or altering of patients' data may easy cause life losses.

(6) Recommendations:

NISTs statement is very short. SaaS CCS should be compliant with various federal regulations used by the government information systems.

The same is applicable to private sector organizations requiring compliance. How that is to be done is the question.

There are the following recommendations:

(6.1) Data protection – Quote: »Analyze the SaaS provider 's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the organization that will be using the subscribed SaaS application.«

This recommendation actually contradicts NIST's opinion that cloud providers are not likely to give customers access to cloud software internals. So, how to analyze anything without the complete documentation of the provider 's data protection architecture or an on-site audit?

(6.2) Client device/application protection - In short NIST recommends to protect your web browser without any advising how to do that.

(6.3) Encryption - Very obvious recommendations: To use data encryption, secure keys, etc.

(6.4) Secure data deletion - Providers should offer a mechanism for the reliable deleting of data on customer 's request. Here NIST touches the very important matter of privacy protection control by data retention.

Ways and means of such a process in a »cloud« are not yet developed. We have considered in our conceptual work (M. A. Utin and D. Utin 2012a) a framework for data retention and gave some practical recommendations.

However, it is far, far from any implementation yet.

Platform-as-a-Service Cloud Environments (PaaS) (Section 6)

In this PaaS section NIST generally follows its previous structure of Section 5 (SaaS):

(1) Abstract interaction dynamics – where the development environment is added, i.e. it is a modification of SaaS.

(2) Software stack and providers/consumers scope of control – where »middleware« is added to the development environment.

(3) Benefits – are very similar to what is considered in SaaS above.

(4)Issues and concerns – very similar to SaaS, plus the lack of portability between PaaS »clouds«, and that is also no news at all.

(5) Candidate applications classes – see SaaS.

(6) Recommendations – very like the ones for SaaS but with some extra flavour: the consideration of a development environment in a cloud. But really nothing new:

By the similarity of the PaaS features, NIST unintentionally confirms our opinion that there is no difference between SaaS and PaaS, both are just hosting services.

NIST did not find anything really significant in PaaS comparing to SaaS to justify a separate consideration of two different models.

Infrastructure-as-a-Service Cloud Environments (IaaS) (Section 7)

NIST considers IaaS as a virtual only environment, where hardware and hypervisor levels are controlled by a service provider. However, instead of referring to the standard Virtual Machine (VM) model and a virtual network of hosts, NIST introduces a new model of IaaS infrastructure which has three layers – Cloud

Manager, Cluster Manager, and Computer Manager (Section 7.3 Operational View, figure 17).

The rationale behind this model, named Logical Cloud Architecture, is questionable.

First of all, computer clusters (even Logical) do not have Cluster Manager above computer level. It would be a single-point-of-failure. Cluster management software exists in each computer node, not on top of them.

The same is true for the Cloud Manager. The failure of such a manager means that the cloud dies. Logical or Not-Logical, such manager should be distributed, and, thus, NISTs Logical Cloud Architecture is contradictory to the essence of a »cloud« as an always surviving hosting environment. We do not see any worth of introducing such »Logical Architecture«, also not to the users of the »cloud«. Does that mean that users will need to manage a »cloud« by three application components – cloud, Cluster and Computer Managers instead of only one like in any other typical virtual environment?

Returning to the document in question we see:

(1) Abstract interaction dynamics – contains VMs only, no infrastructure hosting nodes.

(2) Software stack and provider/consumer scope of control – with added Hypervisor level.

(3) Operational view – which is a new paragraph, but very questionable as we discussed above the concept of Logical IaaS cloud Architecture.

(4) Benefits – NIST lists the following:

(4.1) Full control of computing resources through administrative access to virtual machines

We do not think this is a benefit, because we have the same in any network utilizing virtual and physical hosts. Thus a »cloud«, in this case IaaS, does not decrease network administration work, nor makes it simpler.

(4.2) Flexible, efficient renting of computer hardware

We do not see any advantage here as well. Renting in IaaS requires some time. It may be much easier to create a new virtual machine on a local network than deal with various IaaS administration software in addition to VM management software to add resources. Plus, VM performance degradation is more likely to happen in IaaS than on local network with VMs.

(4.3) Portability, interoperability with legacy applications

We think that it is easier to control old applications on a local network than in a virtual environment, simply, because less software layers are involved, and thus, the chance of incompatibility is less.

(5) Issues and concerns:

(5.1) Network dependence and Browser-based risks and risks remediation

We have discussed that above, and they are native to any »cloud«.

(5.2) Compatibility with legacy security vulnerabilities

Old operating systems and applications may introduce software vulnerabilites; however, on a local virtual network it is much easier to control such situations than in an generally unknown »cloud« environment.

(5.3) Verifying authenticity of an IaaS cloud provider web site

Utilization of shared web resources to run applications always create additional risks.

(5.4) Robustness of VM-level isolation

This is an open issue of any virtualization, which, in the case of the »cloud«, becomes harder to control and resolve.

(5.5) Features for dynamic network configuration for providing isolation

Having multiple customers in the same networking environment creates a possibility of interference, and requires additional resources to control.

(5.6) Data erase practices

Data residue from old customers could be available to new ones, or, when the IaaS virtual network is reconfigured, hosts can still contain old data; that again requires additional efforts to control.

(6) Recommendations for Infrastructure-as-Service:

NIST gives very short recommendations on the following matters which for unknown reason do not coincide with the issues and concerns above:

- Data protection.
- Secure data deletion.
- Administrative access.
- VM migration.
- Virtualization best practices.

The essence of these recommendations is you should acquire detailed technical information from the IaaS provider and act accordingly to it, the NIST virtualization (SP 800-125), and the OVF (Open Virtualization Format aka Open Virtual Machine Format) standard. We think that's kind of ironic: If you are able to resolve NIST's issues and concerns, follow its recommendations and the research of OVF standard proposal, - which is about non-existing- , plus »… emerging cloud use cases...« (see Wikipedia for Open Virtualization Format) then you are ready for a »cloud«!

And what about unprepared »cloud« consumers, who expect a fast to deploy, easy to use, cost effective solution and never heard anything about things like OVF?

Open Issues (Section 8)

NIST document considers issues (yes, yet another set of issues) in the following section:

Computing Performance, Cloud Reliability, Economic Goals, Compliance and Information Security. There are 25 Open Issues total.

Some of them have been considered in previous sections.

Quote: »cloud computing is not a solution for all consumers of IT services, nor is it appropriate for all applications. As an emerging technology, cloud computing contains a number of issues, not all of which are unique to cloud, that are concerns for all IT hosted services.«

We will briefly adress each and explain why it's an open Issue.

(1) Computing performance:

(1.1) Latency - various delays, out of providers' and customers' control; may exist on any WAN, but »cloud« adds uncertainty to it.

(1.2) Off-line data synchronization - a problem working off-line and then syncing data; may exist on any WAN, »cloud« definitely complicates the issue.

(1.3) Scalable programming - not really an CCS issue, relates to distributed computing applications; will require re-development to function and/or utilize »cloud« environment.

In this case NIST mixes distributed processing with CCS, which is pure hosting; it is very unlikely that after all the trouble with moving in a »cloud« customers will start re-developing applications for scalability as well.

(1.4) Data storage management - various issues related to data management, which have been discussed above (for instance – data deletion).

(2) Cloud reliability - NIST identifies it as a function of infrastructure, services and personnel, both of the »cloud« provider and the customer.

(2.1) Network dependence - while applications run in an WAN enterprise environment also depend on networking quality and security, a »cloud« is more troublesome because of its connections to applications over public Internet, not over a private kind of WAN where redundancy can be set up according to the owner's will.

(2.2) Cloud Provider Outages - may happen on any WAN; some uncertainty is added by CCS, in particular because hosting data centers are not really a »cloud« yet and simply cannot provide complete redundancy moving data cross continents. We have seen a case where a data center was shut down by a single power switch during maintenance, and the entire »cloud« went down.

(2.3) Safety – i.e. critical processing; NIST cautiously advises against a »cloudization« of critical systems (government, military, traffic control, etc.). The wide scale experiment of NASA »»Cloud First«« implementation is a perfect example (US General Services Administration 2014b).

(3) Economic goals:

NIST promotes low up-front costs, which is questionable considering the very complex process of moving in a »cloud« - see NIST's opinion above.

(3.1) Risk of business continuity - what if a »cloud« goes bankrupt as it can happen with any business? How to get customer data back?

(3.2) Service agreement evaluation - NIST goes into a short discussion of the automated evaluation of agreements. We think that it is currently unrealistic; more important in agreements are non-standard clauses like protecting customer data as in the paragraph above.

(3.3) Portability of workloads – it means moving data (either pure data or virtual infrastructure) back to the customer premises, or between »clouds«. So far this is a task impossible to implement.

Even in the simplest case – if a data structure in a »cloud« changes, it will require a conversion before moving back. Plus, providers do not want that to happen at all, and clauses for such a possibility usually do not exist in agreements. Giving customers an opportunity of moving between CCS is also questionable, because providers actually want to keep their customers base forever.

(3.4) Interoperability of cloud providers - we discussed above that providers do not want to give customers such opportunities. In addition, various technical aspects decrease the possibility to below zero.

(3.5) Disaster recovery - it depends on the good will of the CCS provider and that is the problem – The promise exists merely on paper. Customers cannot verify how it works.

(4) Compliance – it is the responsibility of the customer to be compliant, no matter if in or out of a »cloud«. There is the list of associated issues below:

(4.1) Lack of visibility - customers simply do not have access to internal security monitoring information. The reason is mostly technical – the provision of SIEM (Security Information and Events Management) service is already difficult to implement locally and for the numerous customers of a »cloud« it is almost impossible. Providers also do not include such clauses of monitoring in agreements.

(4.2) Physical data location - the most important matter is that physical location of data outside of the US territory may be prohibited by regulations; and we can also say that there is no US law which would set up a legal ground for this kind of »data outsourcing«.

(4.3) Jurisdiction and regulation - by various US regulations (HIPAA, GLBA, SOX, PCI DSS, etc.), consumers of CCS are ultimately responsible for the protection of their data, and should aquire compliance assurance from providers; but it is almost impossible to get appropriate documents because providers consider the implementation (including security) as an internal matter and a proprietary information.

(4.4) Support for forensics – the handling of incidents is not a simple matter even in internal networks, and having data outside of legal boundaries creates numerous legal and technical issues like who is dealing with incidents – the consumer or the provider, or both, the accessibility to physical and logical data (audit logs), etc.

(5) Information security: This includes confidentiality, integrity and availabitity; the fundamental issue is, as in (4.3) above, whether consumer can obtain the provider 's assurance that the same or an equivalent level of security controls have been implemented. There is NIST's list of specific matters to consider:

(5.1) Risk of unintended data disclosure - NIST's concern is about keeping sensitive and non-sensitive data in the same »cloud«, and recommends to encrypt sensitive data; however, in other considerations stated above, it was recommended not to keep sensitive data in a cloud, including the risk of incompliance and accessibility to auditing resources.

(5.2) Data privacy – this is a very complex ethical, legal and technical matter, and, as we've discussed above, there is no resolution yet for distributed systems (European Parliament 2012; Ross 2013; M. A. Utin and D. Utin 2012a).

(5.3) System integrity - there are various groups of cloud users (administrators, providers, consumers, etc.), and it's a real challenge to control their access to various cloud resources; we called this challenge »border security« and it was first considered in M. A. Utin and D. Utin 2012b.

(5.4) Multi-tenancy - the problem of the physical sharing of one resource and whether existing logical mechanisms are adequate to protect data; NIST mentions encryption, but it is applicable to data in-rest only.

(5.5) Browsers – NIST discussed numerous times the issue of insecurity of a web browser as a universal tool to access remote resources, but the issue of buggy software will never be resolved.

(5.6) Hardware support for trust – NIST briefly discusses the so called Trusted computing Model, which may, but yet never has been technically used to protect physical and/or virtual computers.

(5.7) Key management – quote: »... It is an open issue on how to use cryptography safely from inside a cloud.« Meaning that NIST cannot give recommendations beyond the known practice of local networks.

We provided this list to demonstrate that customers face a whole lot of issues, some of them »value added« by utilizing CC services. Some (like Physical Data Location and Jurisdiction and Regulation) cannot be resolved yet because they require appropriate legislation. Some are simply inflated by utilizing complex »theoretical« CC models which do not reflect the reality, like the »Interoperability of cloud Providers«.

Needless to say that NISTs opinion is expressed a few times throughout the document – calculate carefully if you want to move to a CCS.

NISTs list of numerous issues (say – problems) proves that: Instead of dealing with LAN/WAN services, a customer needs first to figure out a bunch of unusual or added problems, then he has to do an economic analysis, next re-educate his personnel, then relocate, etc. Wouldn't it be easier and less expensive just to keep the old local infrastructure?

General recommendations (Section 9)

There are five different groups - Management, Data Governance, Security and Reliability, Virtual Machines, and Software and Applications - which contain 30 NIST's recommendations.

Unfortunately, some of them address issues already mentioned, for instance Open Issues, but some of them are completely new.

Such mixed lists do not help the reader to follow the document or to identify the most important issues. We provide a short list of NIST's recommendations (some may already been discussed above) which we think critical including our short comments:

(1) Migrating data to and from a cloud – could be a big problem for customers; a plan should be developed for migration and termination of CCS.

It's good to have a plan, but testing either ingress or egress is nearly impossible, especially its termination. That means a consumer is chained to a provider forever.

(2) Compliance – a customer should thoroughly inform himself about the provider 's security and compliance to make sure that both are adequate.

However, it's very unlikely that a consumer gets permission to dig deep into the providers business, and the verification of the documents of the provider concerning compliance is a questionable process – a real situation might be quite different than the scenario sketched out on paper.

(3) Operating policies – should be operating policies for an external audit, security certification, etc.

It is very unlikely that CCS providers have such policies and processes in place, unless facing an government audit.

(4) Data separation – is about data protection which, within the cloud »concept« was practically not addressed yet.

(5) Data regulation – quote »the consumer is ultimately responsible for all compliances with data-related laws and regulations.«

As we mentioned above, current US security standards like HIPAA, hold providers responsible as well. The customer should »assure« himself, i.e. be certain that security measures are implemented.

The problem is how to get such an »assurance« from providers, and whether documents contain correct information.

(6) Data recovery – quote »Consumers should be able to examine the capabilities of providers with respect to: (1) data backup, (2) archiving, and (3) recovery«.

We don't understand how a customer should be able to »examine« CCS provider premises and processes for these matters, in particular – recovery.

4.2.2 The document analysis conclusion

We would like to return to how NIST explains the purpose of this document (quote):« … to explain the cloud computing technology area in plain terms, and to provide recommendations for information technology decision makers. cloud computing is a developing area and its ultimate strengths and weakness are not yet fully researched, documented and tested. This document gives recommendations on how and when cloud computing is an appropriate tool, and indicates the limits of current knowledge and areas for future analysis.«

NIST definitely tried to do its best, however the »cloud« concept affected the document. It was not possible to explain the area of CCS in plain terms as CCS models are controversial by nature, for instance, »community« clouds. NIST involved additional models to explain the relationship between cloud consumers and providers. However, in the case of IaaS Logical Cloud Architecture, the model is technically questionable. In other cases we don't think they are useful. Having numerous CCS models, NIST needs to figure out features, problems and recommendations for each of them. That makes the document much longer and very repetitive, because issues are often very similar to each other or the same. Recommendations often are simply repeated or slightly modified to fit the issue in question.

The problem is that within CCS models there is no real resolution for such issues, because they were created by the CCS concept. The most practical recommendation was to be very cautious when planning to move into a »cloud«, because of the numerous issues tied to it. We do not think that, after studying this document, an IT decision maker could easy decide to move or not to move into a »cloud«.

Unfortunately the document does not (quote) »… give recommendations on how and when cloud computing is an appropriate tool.« NIST gives various recommendations, but it is not possible to decide »when and how« CCS is appropriate. Moreover, considering numerous security and privacy issues, we can say that the »cloud« is not appropriate.

NIST definitely (quote) »… indicates the limits of current knowledge… « However, what has been considered helps only to decide against IT »cloudization«.

While discussing »clouds«, NIST continuously falls back into the »data center« realm and our terminology of »hosting«, and considers issues limiting the scope of the »data center« as well. This is technically correct, because »clouds« really do not exist yet, and more likely will never appear in the means of distributed computing, at least when it comes to utilizing current models and associated services.

There is one important aspect, which we would like to mention separately, and which will affect US CCS business.

There is no resolution to the matter of private data protection within this SP 800-146 document. The reason is that the US does not have a general law regarding privacy protection similar to the EU General Data Protection Regulation proposal (European Parliament 2012). Thus, NIST does not consider how private data will be protected in distributed computing environment or within a »cloud«. And the implementation of its own NIST's SP 800-53 R4 (Ross 2013) privacy protection controls are not considered as well.

The same is applicable to the CCS providers – no law is pressing them to protect private data, thus no protection gets developed. As a result, US CCS providers will be barred from the EU market as being noncompliant with GDPR and offering no compatible regulation protecting personal data.

In short, our conclusion: The NIST document describes models, services, technology, issues, and gives some advising. It is more discouraging than encouraging about moving into a »cloud«, because there are a lot of associated issues, and some of them prohibit the utilization of CCS for regulated organizations in particular. It's unclear why, with so many concerns and unresolved issues, the US government still continues the FedRAMP CCS program. Maybe because the US general Services Administration (GSA) simply did not read its NIST »cloud« documents?

4.3 NIST SP 800-144 - Guidelines on Security and Privacy in public cloud computing, December, 2011 (current version)

This document is in total 80 pages long: 75 pages of technical text plus 5 appendixes (Jansen and Grance 2011).

4.3.1 The document analysis

NIST on the importance of CCS security: »… The security objectives of an organization are a key factor for decisions about outsourcing information technology services and, in particular, for decisions about transitioning organizational data, applications, and other resources to a public cloud computing environment.«

The purpose of the document (quote) »… The purpose of this document is to provide an overview of public cloud computing and the security and privacy challenges involved. The document discusses the threats, technology risks, and safeguards for public cloud environments, and provides the insight needed to make informed information technology decisions on their treatment.«

While this document is intended to discuss the »public cloud« model only, skipping both the private and the community model considered in SP 800-146 above, there are a few pages returning us to the »deployment« and »service« models.

There is a list of 17 documents (!) in the Executive

Summary, which NIST identifies as involved in the security management process, and thus should be used in a »cloudization« process.

We will discuss two of them below (800-37 R1 and 800-53 R4) as well. However, this list of »cloudization« prerequisites is impressive.

Unfortunately, this document repeats numerous issues, which have been outlined in SP-800-146 – Cloud Computing Synopsis and Recommendations (4.2).

For the consistency of our analysis and references we will list almost all of them as they are in the document, but at the same time trying to eliminate the most repetitive text passages.

Public Cloud Services (Section 3)

This chapter discusses public cloud service in general, and includes some considerations of agreements between a customer and a provider.

It mostly repeats SP 800-146, which we discussed above. By NIST opinion, small organizations (we actually never heard about small government organizations) may benefit from moving to a cloud (from the so called Security and Privacy Upside: staff specialization, platform strength, resource availability, backup and recovery, mobile endpoint, data concentration, etc.) However, there is certainly also a Security and Privacy Downside (system complexity, shared multi-tenant environment, Internet facing services, loss of control, etc.). NIST considers key issues in its next section.

Key security and privacy issues (Section 4)

Quote: »The sections below highlight privacy and security related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.«

(1) Governance – In general, the ability of an organization to control its outsourced information technology. Exploitation and mismanagement could come from both sides – the customer and the provider.

Keeping outsourced technology under control in a public environment may cost more than the service of the original local system.

(2) Compliance – This refers to the responsibility of an organization to operate according to laws and regulations. There are various regulations governing government systems security and privacy .

NIST provides us with short references. One of the most common compliance issues is Data Location. While a local system permits to control where the data is located, the cloud deployment makes such information unavailable, simply because data could be placed anywhere in the »cloud« and its location cannot be identified. Other concerns are about data disclosure and trans-border (international) data flow. There is no federal regulation considering both matters yet. Government regulations also require the capability of Electronic Discovery, meaning that documents should be preserved and if necessary should be readily available for investigation and litigation.

The »cloud« makes that much more difficult because of the Data Location issue mentioned above.

(3) Trust – An organization delegates the control of many security and privacy aspects and thus entrusts it to its provider. However, government organizations (and other regulated organizations as well) are responsible for the protection of its information. NIST considers the following issues:

(3.1) Insider access – Moving data into a »cloud« significantly expands the number of »insiders« having various level of access to critical data, including the personnel of its service provider and other cloud customers.

We called this issue an issue of »border security« and discussed it in (M. A. Utin and D. Utin 2012b).

(3.2) Data ownership – Is the legal question about the original ownership of data; none of the organization's data rights are transferred to the service provider.

(3.3) Composite services – cloud provider may use other services from other providers; liability and performance may become serious issues when third party services are involved.

We see this issue as a legal »terra incognita«, there is no legal experience dealing with multiple legal agreements within one »cloud« service (M. A. Utin and D. Utin 2012b).

Moreover, a »cloud« of a few providers does not technically exist yet.

(3.4) Visibility – The monitoring of its security status and information which has been originally performed by the organization itself locally lies still within the responsibility of the organization when its system is transferred to a »cloud« - but now its capability of monitoring depends on the infrastructure and services of its cloud provider; therefore the monitoring of the customer information system security should be included in the service agreement.

However, as we have discussed, such monitoring is almost impossible to implement.

(3.5) Ancillary data – Customer accounts' information is accumulated by providers in significant numbers, and its compromise may affect millions of customers.

For instance, there was eBay.com case disclosed in the middle of May 2014, which affected the personal information of millions of customers. The protection of accounts may represent a difficult task as it involves both »border security« and »trans-border« issues.

(3.6) Risk management – US federal regulations (OMB documents and FISMA) require service organizations to have the same level of security and protection as federal agencies.

The Risk assessment of a cloud-based federal system is a challenge, if technically and legally is possible at all. The effectiveness of provider's security controls may require an external independent audit, which does not have a federal law to legally support it yet as well.

(4) Architecture – Quote: »Therefore, it is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its life cycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.«

NIST considers in particular Attack Surface, Virtual Network Protection, Virtual Machine Images and Client Side Protection. However, there is nothing new either in its considerations concerning attacks or security controls.

In our talk »Cloud Computing: a new approach to securing personal information and addressing new EU regulations« (M. A. Utin and D. Utin, 2012a) we identified that the utilization of the »cloud« and its security architecture makes it impossible to »decompose and map to a framework of security and privacy controls«. We did what NIST wants, but utilizing a different approach of the »Dynamic Hosting Service« security architecture.

(5) Identity and Access Management (IAM) – When a system moves into a »cloud«, the locally used IAM very likely is to be replaced either by cloud IAM or a mixed system. That presents certain technical challenges because very often a part of the old system should stay local. We see that as »border security« issue of interfering access rights. There is the legal security issue about the users' personal information which could be exploited if moved into a »cloud« . NIST briefly discusses Security Assertion Makeup language (SAML) as a means of exchanging authentication information between »cooperating domains«. However, since such domains do not exist, this discussion is purely theoretical.

(6) Software isolation – there are multi-tenancy issues in CCS.

We have discussed this multiple times above, and classified it as »border security« whether such border is between services, accounts, or databases.

However, NIST does not propose any solution, even in general terms.

(7) Data protection – quote: »Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.«

We think that Data Isolation and Data Sanitization security controls cover only a part of the concerns over data protection. We tend to agree with the position expressed in p.4.2. NIST SP-800-146 that it is not recommendable to move any sensitive information into a cloud.

(8) Availability – NIST discusses the availability of CCS, including temporary outages, prolonged and permanent outages, and denial of service.

As we have already said, situations like (quote) »… If an organization relies on a cloud service for data storage and processing, it must be prepared to carry on mission critical operations without the use of the service for periods when the cloud experiences a serious outage.« should not be possible at all, with the exception of a nuclear war or the blast of super-volcano. NIST assumptions are true for a local data center, not for a distributed system which cannot die because of a power outage or a flood.

(9) Incident response – quote: »The cloud provider 's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration.«

We wrote in (4.4) Support for Forensics that »incident handling is not a simple matter on internal network, and having data outside of legal boundaries creates numerous legal and technical issues like who is handling incidents – the consumer or the provider, or both, accessibility to physical data and logical data (audit logs), etc.«. Again we say that this is very complex technical and legal matter.

(10) Summary of recommendations – NIST provides us with the final list of recommendations which we already addressed above. This one and a half page long list confirms that for the customer to prepare in orderly manner for moving in to a »cloud«requires significant efforts, it does not make life easier for him, nor are economic objectives easy to achieve. As we saw throughout the text, some issues cannot be resolved at all, while some require double or maybe even triple the resources comparing to »local« implementation.

Public Cloud Outsourcing (Section 5)

In this chapter NIST discusses the process of how to move into a »public cloud« in greater details than in the sections discussed above. There are various concerns whether and how to move.

The reality is that (quote):« … The record for traditional information technology outsourcing is mixed with respect to security and privacy, and not consistently done well by federal agencies«.

Unfortunately, NIST does not provide a reference to what »… not consistently done well by federal agencies« exactly means.

The document – SP 800-144 has been officially published in December 2011, and thus, such negative experience was known a while before.

Likely in an attempt to bring order to the process and to improve the record of federal accomplishments, NIST provides us with a How-To-Move- Guide.

Here a short summary with some very brief comments - A detailed analysis, unfortunately, would take too many pages. Readers can refer to the original document in question, if they're looking for details.

(1) General concerns: There are the following issues:

(1.1) Inadequate policies and practices

(1.2) Weak confidentiality and integrity sureties

(1.3) Weak availability sureties

(1.4) Principal-Agent problem

(1.5) Attenuation of expertise

(1.6) FIPS 199 and FIPS 200 are pertinent to all stages of the process

NIST also provides the list of 15 SP 800 documents, which should be considered for detailed guidelines (!).

(2) Preliminary activities:

As first step in outsourcing, customers need to plan these To-Be-Done activities:

(2.1) Specify requirements - NIST lists 19 requirements, which customer should develop (personnel, regulatory, service availability, etc.)

(2.2) Assess security and privacy risks - Such risks have been discussed above and include the following (quote): «… factors such as the service model involved, the purpose and scope of the service, the types and level of access needed by the provider and proposed for use between the organizational computing environment and provider services, the service duration and dependencies, and the strength of protection offered via the security controls available from the cloud provider » and numerous others:

(2.2.1) Personal Identifiable Information evaluation – NIST provides a list with 6 categories (law enforcement and investigation, system security information, licensed source code, etc.), but each customer is likely to have his own list.

(2.2.2) A list of 7 technology areas to review concerning risk analysis – logical data isolation, backup and recovery, capabilities and processes for electronic discovery, etc.

(2.3) Assess the competency of the cloud provider according to the following list - we think that matter is important, and all 9 items are quoted below:

(2.3.1) Experience and technical expertise of personnel

(2.3.2) Vetting process personnel undergo

(2.3.3) Quality and frequency of security and privacy awareness training provided to personnel

(2.3.4) Account management practices and accountability

(2.3.5) Type and effectiveness of the security services provided and underlying mechanisms used

(2.3.6) The adoption rate of new technologies

(2.3.7) Change management procedures and processes

(2.3.8) Cloud providers track record

(2.3.9) The ability of the cloud provider to meet the organizations security and privacy policy, procedures, and regulatory compliance needs.

Our question: Is it possible to get such information from the CCS provider, for instance, the first one about the -»Experience and technical expertise of personnel«?

While the list is logical concerning the risk estimate, the first problem is to collect such information, before it's possible to develop a method of how to estimate the risk. We simply do not see how this could be done.

(2.4) Initiating and coincident activities. NISTs recommended process includes the following activities:

(2.4.1) Establish contractual obligations (10 items):

(2.4.1.1) A detailed description of the service environment, including facility locations and applicable security requirements

(2.4.1.2) Policies, procedures, and standards, including vetting and management of staff

(2.4.1.3) Predefined service levels and associated costs

(2.4.1.4) The process for assessing the cloud providers compliance with the service level agreement, including independent audits and testing.

(2.4.1.5) Specific remedies for harm caused or noncompliance by the cloud provider

(2.4.1.6) Period of performance and due dates for any delivery

(2.4.1.7) Cloud providers points of interface with the organization

(2.4.1.8) Organizations responsibilities for providing relevant information and resources to the cloud provider

(2.4.1.9) Procedures, protections, and restrictions for collocating or commingling organizational data and for handling sensitive data

(2.4.1.10) The cloud providers obligations upon contract termination, such as the return and expunging of organizational data

(2.4.2) The following areas should be totally clarified:

(2.4.2.1) Ownership rights over data

(2.4.2.2) Locus of organizational data within the cloud environment

(2.4.2.3) Security and privacy performance visibility

(2.4.2.4) Service availability and contingency options

(2.4.2.5) Data backup and recovery

(2.4.2.6) Incident response coordination and information sharing

(2.4.2.7) Disaster recovery

(2.4.3) Regularly Assess performance of the cloud provider – NIST recommends a periodical review of the performance and the quality of the CCS provider.

While some tasks could be technically done (we skip the discussion of organizational hurdles), others are extremely complex from both perspectives, for instance – »The process for assessing the cloud providers compliance with the service level agreement, including independent audits and testing«.

(2.5) Conclusive activities: The following activities are expected when a customer is going to terminate cloud service, or moving to another one, etc. thus entering the final stage and the closing of his current contract:

(2.5.1) Reaffirm contractual obligations

(2.5.2) Eliminate electronic access rights

(2.5.3) Recover organizational resources and data.

As we have discussed above so far this is near impossible to do – customer do not have an environment where to put the data which will be recovered from a »cloud«.

It means to re-implement it in great details, basically mirroring the CCS infrastructure and get personnel ready to fix all associated problems in very short time and without any real infrastructure support experience.

Simply put, if an organization has moved into a »cloud« it is forever.

(2.6) Summary of recommendations

NIST provides a table which lists three areas and activities we considered above.

Conclusion (Section 6)

We provide below a few quotes representing NISTs conclusive opinion with our short comments:

(1) »Emphasis on the cost and performance benefits of public cloud computing should be balanced with the fundamental security and privacy concerns federal agencies and organizations have with these computing environments. Many of the features that make cloud computing attractive can also be at odds with traditional security models and controls. Several critical pieces of technology, such as a solution for federated trust, are not yet fully realized, impinging on successful cloud computing deployments.«

The problem is the »balance« between costs and security, because there is no explanation how to achieve it. NIST does not clarify anything on that matter.

(2) »Accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the organization to fulfill. Federal agencies must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization.«

Unfortunately, this requirement gets practically ignored by both government and commercial organizations as soon as they start to outsource their IT and information security. We have seen numerous examples, for example the NASA audit failure (NASA Office of Inspector General 2013).

(3) »Assessing and managing risk in cloud computing systems requires continuous monitoring of the security state of the system and can prove challenging, since significant portions of the computing environment are under the control of the cloud provider and likely beyond the organization's purview.«

As we've discussed above, this is a problem, almost impossible to resolve. The implementation of monitoring for multiple customers would require multiple SIEMs, and thus significant resources. The implementation of one SIEM for multiple »cloud« customers is yet unheard of, and it will be definitely challenging to consider a shared environment for sensitive data.

(4) « . . . Eventually having to displace some systems to another public cloud is a distinct possibility that federal agencies and other organizations must not overlook.«

We doubt that »cloud interconnectivity« will be implemented utilizing »cloud« concept and models. In addition, each provider tends to keep current customers chained to its services. An »open cloud« concept will require new standards and protocols, which nobody is yet interested in.

4.3.2 The document analysis conclusion

The first and very interesting distinction is that the document considers »public cloud«, i.e. hosting service only. That reflects the fact, that, while numerous models of CCS exist, practically only one is in use, and that is the well-known hosting service. What is actually hosted as application – a virtual network or a financial application – is not important. Thus, whatever US government is going to do in a »cloud, is just outsourcing to a hosting service.

»Cloudization«, in a form of various and useless models, did not affect this SP 800-144 document – it is thorough and logical. While we question some of NISTs recommendations (a few are simply unrealistic), the entire document provides us with a logical framework – a roadmap for outsourcing to hosting services. Whether it is possible to act upon it is different question.

NIST is very cautious in advising whether to move in to a »cloud« or not. Fortunately, the people who wrote the document do understand the complexity of moving information systems into a completely different environment, in particular government systems. Initial costs of moving in a »cloud« (see all preparation activties above) will be never compensated by any savings during the systems lifecycle.

It is very likely that, after carefully reading the document (our analysis also could be used) and seeing all issues, considerations, planned activities, lists of required documents, real uncertainty in working with CCS provider, etc., perspective customer will skip the

»cloud« idea. The carefully crafted NIST plan of implementation is almost impossible to implement.

In short: Hosting service, i.e. public cloud, is good for hosting web sites or to implement an Internet shop using the providers development and payment tools, but do not even think about it if your data is personal or confidential information. Read NISTs documents first.

In a better future, if a universal personal data protection law with following acts, standards, protocols, etc. is enacted, hosting service could be made compliant and controlled. Such hosting process should go from compliance and security top to technical implementation bottom. Currently, »cloudization« is completely different – building a data center first and then think how to create a compliance process. It did not work so far, and we will see below why.

4.4 NIST SP 800-37 R1 – Guide for Applying the Risk Management Framework to Federal Information Systems, February, 2010 (current version)

There are two NIST documents related to Risk Management (RM) - NIST SP 800-39 – Managing Information Security Risks, March, 2011 and SP 800-37 R1.

We skip the first document, because it provides us only with a very general consideration of the RM process, and does not contain important practical advise for us.

Below we'll consider SP 800-37 and how it could help us with the identification of »cloud« risks (Ross and Johnson; 2010).

4.4.1 The document analysis

The document is about organizing risk management inside of an organization. Unfortunately it contains only a few very general statements, most of them we have already seen in NIST SP-800-144.

Concerning distributed systems, NISTs analysis is very brief and considers the risks in distributed computing systems only in short, in Appendix I «Security controls in external environments«.

NIST states that:

(1) Organizations are responsible and accountable for the risk incurred by the use of services provided by external providers and address this risk by implementing compensating controls.

We have seen that in other NIST documents above.

(2) FISMA and OMB documents require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies.

The same should be applicable to the private sector if an organization deals with confidential or regulated information.

That is a statement well-known to us as well.

(3) Organizations require that an appropriate chain of trust has to be established with external service providers when dealing with the many issues associated with information system security.

A chain of trust requires that the organization establishes and retains a level of confidence that each participating service provider in the potentially complex consumer-provider relationship delivers adequate protection for the services rendered to the organization.

NIST does not consider risks associated with hosting service type (or CCS) specifics when customer data is transferred outside of the hosting service.

Our short analysis of service risks is represented in Table 3.

Application and Development level, i.e. SaaS and PaaS, may transfer customer data between distributed hosts: thus there is a risk associated with such a process, and should be addresses by privacy and security protection controls. Virtual network service (NaaS) and Network hosting (IaaS) can transfer data only between hosts, because both are software implementations of a network; customer data will stay inside a virtual network (NaaS) or infrastructure (IaaS) .

4.4.2 The document analysis conclusion

Our conclusion reflects the very limited scope of the risk analysis of the document in question.

Organizations are accountable for risks associated with external (i.e. hosting or »cloud«) services and should meet certain security requirements; however, that has been discussed in other documents before.

The »Chain of Trust« concept is new in the consideration of legally bound distributed computing systems in NIST documents; independently we developed a better term explaining such bindings in (M. A. Utin and D. Utin 2012b) – »Delegation of Trust«. It identifies the dynamic legal process of moving trust between distributed nodes, thus establishing a legal relationship based on mutual agreements and information sharing.

This document does not consider risks associated with the type of service. As we identified in the Table 3, two services involve additional external data transfer risks.

Conclusion: this is a pure framework managerial document. NIST provides a very limited - almost none- analysis of risks in CCS even compared to SP 800-144.

Therefore, there is no official standard representing the methodology of estimating and managing risks in a distributed computing system.

CCS Model	Service name	Hosting service name
NaaS	Network as a service	Dynamic Virtual network hosting
IaaS	Infrastructure as a Service	Dynamic Network hosting
PaaS	Platform as a Service	Dynamic Development hosting
SaaS	Software as a Service	Dynamic Application hosting

CCS Model	Transfer of data	Risks
NaaS	Inside of the service	Local risks
IaaS	Inside of the service	Local risks
PaaS	Inside of the service	Local and external risks
SaaS	Inside or outside of the service	Local and external risks

Table 3: Risks of services

4.5 NIST SP 800-53 R4 - Security and Privacy Controls in Federal Information Systems and Organizations, April 2013

4.5.1 The document analysis

Revision 4 is the final version of document SP 800-53. It has been slightly changed comparing to the draft version released in February, 2012. It has 457 pages in total, three chapters and 10 appendixes (A – J).

The general conceptual part contains of only 63 pages. The appendixes D, E, F and J are related to security controls with detailed catalogs of security controls in Appendix F (243 controls) and 26 privacy controls in Appendix J (Ross 2013).

The most significant difference, from our perspective, between the previous Release 3 and the current Release 4 is that NIST now tries to address distributed systems and privacy controls. However, the word »cloud« appears only three times in the document – twice in Appendix D and once in Appendix J.

NIST intentionally avoids labeling any security and privacy controls »for cloud« , thus leaving such decision making to the readers of the document.

This difficult task we resolved for privacy controls in Appendix J (M. A. Utin and D. Utin 2012a) while working on the research of privacy protection in the GDPR (European Parliament 2012).

The SP 800-53 R4 document did not exist when the FedRAMP »cloudization« program was under development. So FedRAMP, which is in implementation now, uses an incorrect outdated list of security controls.

Logically, it should have been the other way round: First a list of security controls for »cloud« services, and then a federal program implementing such services.

4.5.2 The document analysis conclusion

Our analysis was extremely brief considering the volume of the document, because NIST did not include any recommendations for utilization of security and privacy controls in distributed (or »cloud«) information systems, including federal information systems.

From our point of view, NIST should include the consideration of applicability of SP-800-53 R4 security and privacy controls to its own eight (currently 9) »cloud« models. The organization should prove that models and security controls can co-exist. FedRAMP is using an old version of SP-800-53 which definitely affects the programs documents. Even considering NISTs self-escape from »cloud« advising, the new document has a definite value and can be successfully used for security and privacy implementation.

5 The US Federal CCS FedRAMP program

It started as no program of such magnitude should start, and continues in controversy.

There were several influencing factors, which defined its fate, and may influence the future of the US government information technology as well:

1. US government outsources whatever is possible to outsource, expecting to decrease, or, at least not to increase, federal spending.

2. The short Term US presidency forming a desire to quickly do something different and remarkable to be remembered.

3. Enormous marketing pressure from US IT industry promoting whatever is new on market, and currently this is CCS (by HP, IBM, Intel, Microsoft, etc.).

4. Personalities of the president's office staff.

5. Etc., so you may extend this list

5.1 How the »cloudization« reform has started

The US government program of »cloudization« of federal information systems officially started on December 9, 2010 when the Office of Management and Budget (OMB) released an ambitious document called »25 Points Implementation Plan to Reform Federal Information Technology Management« (Kundra 2010). The author was the then US federal CIO Vivek Kundra (following – the CIO) (Wikipedia 2014b).

The header of the plan says it all -»Implementation Plan«, neither concept nor research. It is nothing less than a deep reform, or a revolution, of the entire federal IT management and infrastructure. Both were considered outdated and inefficient, thus requiring complete rebuilding using new principals of management. The plan did not include any financial information while promising to cut the federal budget. However, »cloudization« was not enough, the CIO wanted to rebuild the IT projects funding system (!) in Point 20 »Work with Congress to consolidate commodity IT spending under Agency CIO«. The Plan has other »revolutionary« managerial ideas, it is in its entirety a remarkable adventurous document.

And the Federal government was ready to implement that in 25 steps.

In fact, the process of »cloudization« started almost officially on September 15, 2009, more than one year before the official release of the »25 Points« plan (Kundra 2010).

Speaking at the NASA Ames Research Center (Terdiman 2009), the CIO unveiled the plan about (quote) »...administration's first formal efforts to roll out a broad system designed to leverage existing infrastructure and in the process, slash federal spending on information technology, especially expensive data centers«. According to the CIO, the federal government back then had an IT budget of $76 billion, of which more than $19 billion was spent on infrastructure alone. And within that system, he said, the government "has been building data center after data center," resulting in an environment in which the Department of Homeland Security alone, for example, has 23 data centers.«

As we see from the news reports (Terdiman 2009), the starting point was completely economical. However, the following »25 Points« did not provide any financial information concerning the current budget, and how expected savings should occur. Any concerns about information security, which would require additional resources and budget, were simply ignored as well. According to plan, its author expected to finish his revolutionary job in 2015. We have the following dates of important events outlining the beginning of federal »cloudization« process:

- March 2009 – the CIO started his federal job at the General Services Administration (GSA) office
- September 2009 – Announcement of CCS government program
- December 2010 – Introduction of the »25 Points Implementation Plan« and the announcement of resignation from CIO office within 7 months (!)
- February 2011 – NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing draft document
- September 2011 – SP 800-145 The NIST Definition of Cloud Computing Document
- December 2011 – SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- February 2012 – FedRAMP Concept of Operations (CONOPS) (US General Services Administration 2012)
- May 2012 – SP 800-146 Cloud Computing Synopsis and Recommendations document
- April 2013 – SP 800-53 R4 Security and Privacy Controls (Ross 2013) document

As you can see the CIO announced an extremely ambitious program with his »25 Points Implementation Plan« without ANY official supporting standards from NIST. The draft version of SP 800-144 has been published three months after the »25 Points Plan«, and the most important paper, SP 800-146, more than one year later. FedRAMP CONOPS was also published one year and two months before SP 800-53 R4 with its »cloud« security controls.

What was the source of such confidence of the CIO in promoting CCS? We will see below.

5.2 The CCS promoter

Who gets to the upper level government offices defines what happens next. The US is not an exclusion. While we prefer not to study personalities of former and current US management, our research requires comparing some dates and facts to understand the background of the »cloudization« and the FedRAMP program.

The program has been initiated by the CIO (Wikipedia 2014b), based on his previous experience working for the state government in Virginia and DC. He announced the program to completely rebuild the US federal IT after only 6 months in the GSA office.

5.2.1 A short profile of the federal CIO

1. He was born in New Delhi, India in October, 1974
2. In 1985 he moved from Tanzania to the US, Washington DC with his parents
3. Education:
    - University of Maryland, College Park, degree in Psychology
    - University of Maryland University College – MA in Information Technology
    - University of Virginia Sorensen Institute for Political leadership, graduated (Thus, he had only two years of IT education before the following IT management jobs)
4. Director of Infrastructure Technology, Arlington County, Virginia – September, 2001 (26 years old)
5. Assistant Secretary of Commerce and Technology, Virginia (dual cabinet role) - January 2006
6. Chief Technology Officer for the District of Columbia – March, 2007
7. First Chief Information Officer of the US – March, 2009
8. On March 13, 2009, the federal CIO was placed on indefinite leave following an FBI raid on his former DC office and the arrest of two individuals in relation to a bribery investigation; they were later convicted. He returned to duties after five days - there were no findings of wrongdoing on his part.
9. Resigned from his office in August, 2011 after two and a half years, accepting academic fellowship at Harvard University (president Obama graduated from Harvard Law School)
10. Joins Salesforce.com in January 2012 as Executive Vice President of Emerging Markets (this company has been awarded GSA five-year 28 million contract in August 2011 (Washington Technology 2011)

Conclusion: The CIOs career was develeoping noticeably fast, but ended up abruptly moving him from a very prestigious role to Harvard University for a few months and next to the CCS company executive position. This company was his vendor on an email project (see below) and also got a federal 28 million contract from his GSA office exactly at the same time he left the office (Washington Technology 2011).

Neither his education, nor his federal CIO experience before (see below) shows any traces of Information Security. He was not required to implement federal security regulations while working for the Virginia and DC governments (Wikipedia 2014b).

5.2.2 IT projects in DC and around

The work of the federal CIO for both the state of Virginia and DC was considered as very successful (Wikipedia 2014b). The focus was on the automation of local government functions and activities utilizing publicly available web applications, for instance, such projects like »Apps for Democracy«. The DC government claimed the saving of millions of dollars in internal and operational costs resulting from this projects. Mr. Kundra was recognized for his innovative work in project management systems for the local government and the use of web applications hosting services, for instance, utilizing Google Apps that (claimed but not independently confirmed) saved millions of dollars comparing to alternative solutions. His utilization of web application hosting attracted numerous followers, now convinced that such technology can decrease operational and management costs. Again, there were no publicly available documents supporting these claims.

Conclusion: Ad-hock based projects, which have been implemented in short time and definitely without any serious consideration of aspects of information security, attracted numerous followers and created a sense that web application hosting »cloud« services can be used widely and for any IT system. Of course, all these projects were not based on the federal Certification and Accreditation (C&A) information security process requirements (NIST 800-37 R1 Guide for Applying the Risk Management Framework to Federal Information Systems). And cost savings from utilization of web application hosting were not confirmed by independent financial audits.

5.2.3 Federal CIO

As a new federal CIO he continued the utilization of web application hosting in addition to his various administrative responsibilities and plans of rebuilding both the government IT and its budgeting system. His projects included the launch of the Data.gov platform in May, 2009 to provide public access to raw datasets generated by the Executive government branch, and in June 2009 the IT Dashboard to track all government spending on federal IT systems and projects. His major »cloud« related project was moving GSA to the »Google Apps for Government« service and the Salesforce.com platform in July 2011.

Here is the quote from Wikipedia (2014b): »The first major cloud project during his tenure was GSAs migration of e-mail/Lotus Notes to the Gmail and Salesforce.com platform. GSA awarded a contract for e-mail in December 2010 and a five-year contract to Salesforce in August 2011 (see Washington Technology (2011))... In September 2012 the GSA Inspector General Report (see Office of Audits, Office of Inspector General, US General Services Administration (2012)) found the savings and cost analysis not verifiable and recommended GSA update its cost analysis. GSA office of CIO was unable to provide documentation supporting its analysis regarding the initial projected savings for government staffing and contractor support.

Quote: »The audit found that the agency could neither verify those savings nor clearly determine if the cloud migration is meeting agency expectations despite initial claims that indicated 50% cost savings.«

Conclusion: Local and then federal government projects utilizing web application hosting were not adequate to claim an experience in utilizing CCS for various IT systems. Definitely the biggest project was to initiate the conversion of the entire US government IT system to CCS. However, it is not clear why this successful CIO announced the conversion plan and his future resignation at the same time, after less than two years of being part of the GSA office. The financial GSA audit of moving GSA email to Google Apps and Salesforce.com did not find any initial documentation supporting the claimed savings of 50%, nor can the saving be verified.

5.2.4 Conclusion

- We were interested to know some details about the first federal CIO of Obamas administration tenure because he initiated the complete reconstruction of the federal IT with the intention of moving it into a »cloud«.

  He successfully developed a few systems for Virginia and DC local government utilizing web application hosting. However, there were no independent audits confirming claims of cost saving in any of these projects.
- It looks like the Obama administrations search for options to save costs and the CIOs reputation as an innovative and money saving person brought him into office. After only 6 month in office at the NASA Ames Research center, he announced his program to re-build the federal IT, and move it into a »cloud«
- NASA went into »cloudization« not by its own will. The most technically advanced unit with experienced IT personnel, was chosen as testing ground to satisfy the ambitions of the new president and his CIO.

  Definitely, this was a politically motivated decision – a show case, like the entire »Cloud First« project.
- The first project of moving GSA to a »cloud« email service did not pass the financial audit in 2012. Claims of cost savings were not supported by initial documentation, neither were such savings identified.
- Initiated by the federal CIO his »cloudization« programs »Cloud First« and FedRAMP, were not supported by any research documentation or NIST standards, nor had he any adequate exper-

ience in such high magnitude projects.

5.3 FedRAMP initiating the »25 Points Plan«

This plan was named »25 Points Implementation Plan to Reform Federal Information Technology Management« and is not about feasibility research, but a To-Do implementation list.

The document has 40 pages. It indeed has 25 Point, i.e. short paragraphs briefly explaining what the author means.

5.3.1 Security and the »25 Points Plan«

We searched through the 40 pages document for »security« associated topics. Here is what we found:

(1) Page 9 – the plan is aimed to »increase the overall security posture of the government«.

Thus, there seems to be no doubt that moving in to a »cloud« means better security.

(2) Page 11 – Quote: »Within the next six months, the Federal CIO will publish a strategy to accelerate the safe and secure adoption of cloud computing across the government. The National Institute of Standards and Technology (NIST) will facilitate and lead the development of standards for security, interoperability, and portability. ... While cloud computing services are currently being used, experts cite security, interoperability, and portability as major barriers to further adoption. The expectation is that standards will shorten the adoption cycle, enabling cost savings and an increased ability to quickly create and deploy enterprise applications.«

The hopes of the CIO did not come true. Our analysis of NIST standards shows that in fact NIST does not promise to »shorten the adoption cycle, enabling cost savings and an increased ability to quickly create and deploy enterprise applications.« Throughout the entire document the CIO did not find space to address security concerns. This means that he did not have any concerns related to security and had not seen any problem in moving fast into CCS. There's a very brief statement concerning security: »... experts cite security, interoperability, and portability as major barriers to further adoption... « That is simply not adequate for such a program.

(3) This is how the author of the document saw the future (p.37): »The future picture for Federal Government IT is exciting. IT enables better service delivery, enhanced collaboration with citizens, and dramatically lower costs. We must get rid of the waste and inefficiencies in our systems. Outdated technologies and information systems undermine our efficiency and threaten our security.«

We will see soon what the NASA's own audit discovered, and the auditors definitely found this picture exciting.

5.3.2 Some ideas of the plan

(1) The shift to the »Cloud First« policy - each agency will identify three »must move« services within three months, and move one of those services to the cloud within 12 months, the remaining two within 18 months.

However, what if an agency does not have anything for »cloudization«?

(2) Reduce number of federal data centers by at least 800 by 2015.

Where would they go was not explained. Will datacenters be simply demolished or sold to the private sector for cheap money?

(3) Quote: »The shift to »light technologies,« that is, cloud services, which can be deployed rapidly, and shared solutions will result in substantial cost savings ... For example, GSA recently entered into a contract to shift email services to the cloud, resulting in a 50% cost reduction over five years – a savings of about $15 million.«

Here the CIO talks about a concrete amount of savings – but the 2012 GSA audit (Office of Audits, Office of Inspector General, US General Services Administration 2012) was not able to confirm $15 million savings from the email project, nor found any documentation supporting this claim.

5.3.3 Conclusion

This »25 Points« plan represents the still widely existing ignorance and incompetence of IT management in matters of information security. The custom of »IT system first, we will add security later« is deeply embedded.

- The »25 Points« plan of how to re-build the entire government IT and move it to utilize commercial web hosting did not contain any consideration of security. The author was unaware of security issues and threats associated with web hosting and sharing resources.
- The reference to future NIST standards outlined the fact that the plan »Cloud First« has been crafted as »IT First«. NIST security recommendations were yet to be developed thus could not be included in the plan.
- The numbers of data centers to shut down and sites mandatory to be transferred to the »cloud« were not explained. The plan is a typical sale of an idea without any reference to supporting research.
- The former CIOs first federal »cloudization« project of moving GSA email to web hosting application services, which is expected to (quote) ». . resulting in a 50% cost reduction over five years – savings of about $15 million« failed to comply according to the government audit. Moreover, no documents supporting the initial claims of savings have been found.

5.4 FedRAMP Concept of Operations (CONOPS) document analysis

FedRAMP was established by OMB memorandum on December 8, 2011. There are various documents supporting the FedRAMP program. They are available on the GSA FedRAMP portal[1] for analysis of the IT management aspects.

The CONOPS document appeared more than one year after the initial »25 Points« plan. We want to check if there were any changes in the initial program according to security management.

5.4.1 The programs security management process

The official version of CONOPS is 1.0 (US General Services Administration 2012) is dated February 7, 2012 and has 47 pages. It is shaped by its time and events: The former federal CIO resigned six months ago, and was working for the federal contractor Salesforce.com CCS provider when this document was published; and NIST SP 800-144 was in effect for three months, warning about security problems in »public cloud« and very uneasy about the whole process of moving into a »cloud«.

In this document the purpose of FedRAMP is identified as (quote): »FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.«

In the CONOPS overview we found that the aspect of information security, initially ignored in the »25 Points« plan finally gets its required attention (quote):

»A key element to successful implementation of cloud computing is a security program that addresses the specific characteristics of cloud computing and provides the level of security commensurate with specific needs to protect government information.«

The following explains the process of moving to CCS - the three final steps are about security management:

1. Federal agency customer – has a requirement for cloud technology that will be deployed into their security environment and is responsible for ensuring FISMA compliance.
2. Cloud Service Provider (CSP) – is willing and able to fulfill agency requirements and to meet security requirements.
3. Joint Authorization Board (JAB) – reviews the security package submitted by the CSP and grants a provisional Authority to Operate (ATO).
4. Third Party Assessor (3PAO) – validates and attests to the quality and compliance of the CSP provided security package.
5. FedRAMP Program Management Office (PMO) – manages the process assessment, authorization, and process of continuous monitoring.

Chapter 3 describes the ongoing assessment and authorization monitoring process (quote): «… For systems with a Provisional Authorization, FedRAMP, in conjunction with DHS, conducts ongoing assessment and authorization (continuous monitoring) activities. Ongoing assessment and authorization (continuous monitoring) determines if the set of deployed security controls continue to be effective over time.«

Chapters 6 and 7 of the document describe the Security Assessments process. We think that there is a significant flaw in this process – it misses the role of a federal agency (customer) in outsourcing its security controls to CSP.

In this process the agency should review almost the final security assessment package, assess its impact and negotiate a contract with CSP, and then grant (or not) the ATO.

»Before cloud« the agency as IT system owner was responsible for the planning and implementation of the security processes in compliance with the government regulations. CONOPS excludes the agency from the participation in initial security controls negotiation with the CSP. CSP and FedRAMP JAB (Joint Authorization Board) will do that for the agency. Therefore, the agency is moved from its original role as system owner being in control of its own security to passive waiting rather than participating in such a process. It means that the agency's input and influence in the process is very limited in the final approval phase. Instead of initiating a talk with CSP and introducing its security plan, the customer has to wait patiently for its final version and can only negotiate afterwards. Somehow CONOPS considers all federal systems as very similar, and sees no need for the system owners knowledge and input in the initial negotiation of controls.

5.4.2 Analysis conclusion

1. CONOPS represents a thoroughly developed plan, which sets the protocol of security management process between the government (customer-agency and FedRAMP management), CSP and the third party assessor. The document identifies responsibilities and activities of all parties. The document is a definite breakthrough comparing to the »25 Points« implementation plan.

2. However, the deficiency of this conceptual document is the role of the customer-agency. By all governmental regulations, it is responsible for secure operations of its systems when local, and assuring secure operations while in a »cloud«. In CONOPS the customer is excluded from the participation in the beginning of the process and has only a say in the final consideration and approval. A phase like assessment and testing by 3PAO does not mitigate the problem.

[1] http://www.gsa.gov/portal/category/102375 r. 2015-10-21

6 Auditing of results of NASA's Implementation of FedRAMP program in progress

According to the GSAs email hosting project audit (Office of Audits, Office of Inspector General, US General Services Administration 2012), results of moving in to a »cloud« can be really surprising.

Quote: « Finding 1: Some aspects of the projected cost saving for the transition cannot be verified because the OCIO has not updated the cost analysis or maintained the supporting documentation.«

It is interesting to see what happened with NASA's »cloudization«, because it was the first agency really testing the implementation of FedRAMP.

6.1 The results of the NASA Inspector General audit »NASA Progress in Adopting cloud-computing Technologies«

NASA is one of the most technically advanced agencies with very sophisticated IT services. Instead of testing the FedRAMP process by slowly moving small agencies and auditing results to confirm that such a process works, the presidential administration decided otherwise. This politically motivated decision created enormous security problems, which have been discovered by the audit (NASA Office of Inspector General 2013) and published on July 29, 2013. The audit did not check the financial part of the project still in progress. We believe that this would bring unsatisfactory results as well, because the process was not tested, involved a lot of resources, lacked coordination, was ad-hoc, etc. and thus required additional time and resources. Concerning the future, it is very likely that significant expenses inside and outside of the agency will occur while fixing security problems, and therefore this will affect the estimated »cloudization« savings.

The following are quotes from the audit report:

(1) »We found that the Agency OCIO was unaware of two of the eight companies providing cloud services to NASA organizations and that two centers had implemented cloud services. In addition, only 3 of 15 NASA organizations surveyed indicated that coordination with the Agency OCIO was required before moving systems and data into public clouds.«

(2) »None of the five contracts came close to meeting recommended best practices. The standard contracts failed to include Federal privacy, IT security, or records management requirements and the individualized service contract failed to address many of the best practices discussed earlier. As a result, the NASA systems and data covered by these five contracts are at risk of compromise, which could adversely affect Agency operations or result in the loss of data. In addition, because none of the contracts specified how a provider 's performance would be measured, reported, or enforced, »

(3) »We reviewed documentation provided by eTouch and RightNow, including systems security and contingency plans, authorization to operate the system, and the results of annual system control tests. We found that NASA's internal and external portal, which includes more than 100 websites, was operating without system security or contingency plans and with an operating authorization that expired in 2010. Even more troubling, a test of security controls on the IT services provided by the NASA Portal had never been undertaken to determine whether the system's controls were implemented correctly.«

So why is NASA still operational beside these security problem? We think because of the agency projects, goals and its reputation around the world. Some sentiments about its mission may affect the desire of the black-hat community to test the US government agency information security posture.

6.2 Conclusion

1. The audit discovered significant security problems in systems moved to a »cloud« and an inconsistent security management process; in particular within the coordination of »cloudization« activities inside the agency. The contracts assessment process (in terms of CONOPS) was inconsistent as well.

2. We believe that the NASA management and the personnel did not implement the NIST SP 800-144 recommendations; otherwise the process of moving to CCS would not have been so fast and would not have such impressive security gaps.

3. We believe that CONOPS's misconception of the »security assessment« process which was led by the service provider and FedRAMP, excluding customer-agency in the beginning of the process, has contributed to multiple NASA FedRAMP implementation problems and thus insecurity.

4. The audit shows significant material supporting the idea of the »cloudization« and lacks the style and purpose of a pure audit. In particular, while not analyzing the financial part of the project, the audit contains some examples and numbers to convince the reader of the economic feasibility of moving to CCS. We consider that as politically motivated promotion of the government's »Cloud First« approach.

5. We believe that problems with moving into a »public cloud« will continue, may become less shocking, but not less affecting the security.

7 Analysis of FedRAMP NIST SP 800-53 R3 security controls

So far we've provided enough analysis of important US government documents to prove our case that the concept of »cloudization« is questionable and insecure. However, we felt that it would be inconclusive to skip FedRAMPs consideration of Security Controls (Virka 2013) . We want to have the complete picture. We thoroughly studied the document in question and decided to include a short description of common issues in our paper rather than provide you with a long list of very similar comments (Ross 2013).

We would like to note that FedRAMP administration issued a «Security Controls Preface« (US General Services Administration 2014a), but, unfortunately, the document does not address any of the questions we have after studying the controls list. Basically, in the context of guidance for security control implementation, it is a useless document.

7.1 Brief analysis

The FedRAMP list contains security controls from the outdated version NIST SP 900-53 R3. The spreadsheet with controls dated 01/06/2012, that is one month before the draft of NIST SP 800-53 R4 has been published. The GSA FedRAMP page under »About FedRAMP« still contains the statement (quote) »...The FedRAMP assessment process is initiated by agencies or cloud service provider (CSPs) beginning a security authorization using the FedRAMP requirements which are FISMA compliant and based on the NIST 800-53 rev3 and initiating work with the FedRAMP PMO.«

While not having separate »cloud« security controls, R4 version nevertheless contains modified controls and recommendations helping to implement them in distributed computing environment. Additionally, this release has its Appendix J with mandatory requirements to implement privacy protection controls.

Why the FedRAMP administration overlooked the new version, which is mandatory to implement, and did not modify its security control list, we don't know - it could be attributed to poor program management.

The security control table has a lot of skipped fields, security controls not recommended for implementation, shortly labeled »None« without any comments.

The table has a very short description of required controls, but there is no explanation why they are required.

Comments should be a part of this document helping users to understand the implementation and management of security processes according to SP 800-53 R4 and other NIST documents, for instance 800-144.

The majority of controls have a statement like this: »Requirement: The service provider defines the list of security functions. The list of functions is approved and accepted by the JAB (Joint Authorization Board).« This is the practical implementation of the »security assessment« concept which we found in CONOPS document, in fact a pure misconception. The »cloud« service provider and FedRAMP JAB (Joint Authorization Board) lead the process of identifying security controls, thus leaving the customer-agency aside. However, the agency is still responsible for security assurance.

It is obvious that NIST's warning that CCS providers tend to limit the access of customer-agencies to their environment internals, i.e. security controls implementation, was basically ignored by CONOPS.

7.2 Analysis conclusion

FedRAMP uses the outdated R3 version of SP800-53, which does not have recommendation for a distributed computing environment, and neither has any recommendations for privacy controls.

The FedRAMP table of security controls offers no explanation why a lot of controls have been excluded, neither explains about the ones included.

CONOPS's misconception of excluding the customer-agency from the »security assessment« process leads to inconsistent security controls where all decision making and implementation is moved to the service provider and JAB (Joint Authorization Board).

8 Our own financial »audit« – NASA budget analysis

NASA's audit of its »cloudization« misses financial objectives. We decided to do our own audit to fill out the gap.

8.1 Analysis of NASA public budget documents

According to NASA Office of Inspector General (2013): »NASA spends about $1.5 billion annually on its portfolio of information technology (IT) assets, which includes more than 550 information systems ... The adoption of cloud-computing technologies has the potential to improve IT service delivery and reduce the costs associated with managing NASA's diverse IT portfolio. Specifically, cloud computing offers the potential for significant cost savings through faster deployment of computing resources, a decreased need to buy hardware or build data centers, and enhanced collaboration capabilities.«

The following information has been taken from www.nasa.gov and Wikipedia. The Table 4 represents the total NASA budget for 2009 – 2014 (projected)

The trace of NASA's total budget (Tab. 4) is pretty flat with some decrease in 2014. However, we can not draw any conclusion concerning planned or existing savings due to the »cloudization« based on total numbers, and need to see the IT budget itemized.

We found detailed NASA IT budget information in the so called »President's Budget Request Summary« documents for 2014 and 2013 (NASA 2013, 2014).

Corresponding tables are presented here, we think that Tables 6, 4 and 5 provide essential information concerning the reality of any NASA savings due to »cloudization«.

Transferring IT services to CCS involves both IT management and Infrastructure budget items. The year 2011 is »pre-cloudization«: Its major document – FedRAMP CONOPS - has been officially published in December, 2011.

In 2011, before »cloudization«, the Infrastructure budget was 54.7 million, and in 2012, when the project started, it rose to 76.0 million. There is more than a 21 million increase in spending. In the beginning of the program it does not look like saving. Unfortunately, we do not have any information for 2013. However, we can compare what was requested and expected further. In 2011 – before »cloud« – the request for 2013 and further was 73.7 million, and in 2012 the budget jumped up to 94.8 - i.e. also 21 million.

By any means moving to a cloud was presented as outsourcing and the utilization of hosting services instead of the internal IT infrastructure. Therefore a planned increase of the budget of Infrastructure can mean anything but savings from »cloudization« - Or the NASA budget is an inconclusive document, which does not represent the agencies debit structure.

One more interesting consideration about savings from the IT budget: For the year 2012 NASA's total budget was 17.7 billion, and its IT budget was 158.5 million. Thus, the IT budget is only 0.9% of the agency budget.

If the »cloudization« saves, say 30% of the IT budget, it will be less than 0.3% of the entire budget. Does it make any sense to completely rebuild NASA's IT and to put operations of such an agency at risk to save 0.3%?

8.2 The conclusion of the analysis

We used publicly available NASA budget information. A detailed budget for 2013 is not yet available. However, we were able to identify that the government does not plan any decrease in NASA IT budget positions associated with moving in to a »cloud«. Moreover, we see an increase of 21 million of spending on IT infrastructure. So, where is the economical advantage of »cloudization«?

When it comes to budget savings we do not see any reason for NASA to move its IT into a »cloud« , because the total IT budget is only around 0.9% of NASA's total budget, and any savings in IT infrastructure will be unnoticeable comparing to the whole sum of the agency budget.

9 Research conclusion

Two fundamental models of cloud computing – the Service and the Deployment Model – are useless; the hosting nature of CC is easier and better explained using traditional hosting terminology; four deployment models are useless for customers because their nature of networking can be easier explained in old LAN/WAN and outsourcing terms.

The models of community and hybrid deployment are nonsense legally, because a »community« is not a legal entity and cannot participate in contracts and other agreements; however, NIST used the models in its SP 800 documents while broadly discussing the legal side (i.e. contracts and SLAs) of CC services. Only one of three »cloud« related NIST documents – SP 800-144 - discusses CC security seriously and thoroughly; however, only for one deployment model – the »public cloud«, which is simply a hosting service; the other three models were intentionally skipped and not discussed. We believe because of the extreme complexity of such an analysis.

Our thorough analysis of NIST SP 800-144 (Guidelines on Security and Privacy in public cloud computing) shows that the proposed process of transferring traditional IT services into a »cloud« is very complex and requires the consideration of various factors, the creation of a transition processes, the consideration of dozens of documents, etc.; the transition processes should take years and should be very carefully planned.

NISTs advice, listed issues, recommended activities, etc. mean, in plain language: Do NOT Go »cloud« unless your service is very simple and you do not have any regulated information like personal, private, confidential, etc. information, which protection is required by laws.

NIST, while claiming that the new Release 4 of SP 800-53 contains recommendations concerning »cloud« security controls, in fact does not provide a list of such controls for security and privacy. Also neither recommendations and/or comments are provided - Users of SP 800-53 have to consider the application of controls to CC models themselves.

NIST SP 800-37A (Guide for Applying the Risk Management Framework) does not provide any real recommendations concerning risks in distributed computing or CC/CCS environment.

The federal program of moving all possible IT services into a »cloud« – »Cloud First« – was a political campaign to save IT costs without any serious analysis how to do that; it was originated by the then federal CIO without any real plan and experience; the first federal project of moving GSA email in Amazon and Salesforce »cloud« later failed the financial audit of the GSA .

The initial »cloudization« plan – »25 Points« - was a pure IT plan without any security considerations; it did not address any security concerns and proposed nothing concerning information security.

The FedRAMP program finally issued a document called Concept of Operations (CONOPS), which addressed information security; however it did not use the updated NIST documents, including SP 800-53

Year	2009	2010	2011	2012	2013	2014
Budget, billions	17.78	18.72	18.45	17.77	17.7	16.6

Table 4: NASA budget for 2009 – 2014 years

R4;

FedRAMP is still using outdated security controls. The FedRAMP CONOPS document implies very serious misconceptions – it excludes the system owner (i.e. the »cloud« customer-agency) from participation and negotiation of CCS security controls in the beginning of the transition project; its participation only in the final stage will then be formal and ineffective.

FedRAMPs issued list of cloud applicable security controls (based on the outdated NIST document SP 800-53) does not provide any comments or explanations why some security controls were included and others excluded. Additionally it is also affected by the CONOPS misconception mentioned above – the security decision making is outsourced to the cloud provider.

In the very beginning of »cloudization« NASA has been chosen as the testing site for the FedRAMP program; there is no doubt that this was a politically motivated and technically insane decision of the presidents administration and the then federal CIO in particular.

In 2013 NASA's internal Office of Inspector General (OIG) found multiple security problems in the current implementation of the agency's »cloudization«. It failed to implement security processes as required by OMB, FISMA, and NIST US government documents.

While NIST's OIG either was not able to analyze the NSA budget - or did not plan for, or was trying to limit the impact of its audit - we analyzed the NASA budget looking for any appearing or planned savings of the agency's IT.

We found that the IT infrastructure budget has actually increased for 21 million and will stay on this level; how the budget increase corresponds to the expected savings due to »cloudization« we cannot explain.

10 Final Research Note

As we identified in the beginning of this article, we started the research to clarify if the US government's »Cloud First« initiative and the »cloud« based program FedRAMP confirms that the »cloudization« is an appropriate technological solution for the processing of sensitive information, and if it has saved or will save taxpayers' money as well.

We proved that »cloud computing« is neither computing technology, nor a new concept. Its nothing but a pure marketing attempt to sell the good old data center based application hosting. Federal documents supporting FedRAMP have numerous issues. SP 800 - NISTs attempt to lay down »cloud« utilization documents - failed as well. It includes only one useful document – SP 800 -144. However, the document states that moving in a »cloud« is a very complex process, with numerous technology and security issues, and that the economical advantage of such a move is unclear.

»Cloud First« and the following FedRAMP program started disorderly and were purely political motivated. The rush to implement and the utilization of the NASA information technology system to test the »cloudization« process were insane and ended up in mismanagement and numerous security problems. The economical advantage of the»cloudization« has not been confirmed, and, by our research, cannot be found in the NASA budgetary documents. There is nothing new in the utilization of data centers for application hosting services, but keeping, processing and moving private and confidential data in distributed computing systems requires a completely different approach and implementation.

11 About the Author

Mikhail A. Utin completed his basic engineering education in 1975 in Computer Science and Electrical Engineering. His career in Russia included working for several research and engineering organizations. Doctorate / PhD in Computer Science (1988) from then Academy of Science of the USSR. From 1988 to 1990 he founded an information technology company and successfully worked in the emerging Russia's private sector. He had several USSR patents and published numerous articles. Immigrated in the US with family in 1990 to escape from political turmoil and hoping to continuing his professional career. Worked in the US in information technology and information security for numerous companies and organizations including contracting for US government DoN and DoT. Together with colleagues he formed the private company Rubos, Inc. for IT security consulting and research in 1998. The company is a member of ISSAs New England chapter. (ISC)2 certified professional for seven years. Published articles on the Internet and in professional journals, and reviews articles submitted to the (ISC)2 Information Security Journal: A Global Perspective. Current research focus on information security governance, regulations and management, and the relationship between regulations, technology, business activities and businesses' security status. Most of the research is pioneering work never discussed by the information security community.

	2011 Actual	2012 Estimate	2013 Request	2014∗	2015∗	2016∗	2017∗
Agency IT Services	145.0	159.1	152.0	152.0	152.0	152.0	152.0
- IT Management	15.0	14.6	10.5	10.5	10.5	10.5	10.5
- Applications	75.3	67.8	67.8	67.8	67.8	67.8	67.8
- Infrastructure	54.7	76.6	73.7	73.7	73.7	73.7	73.7

Table 5: NASA IT detailed budget 2011 – 2017 (million dollars) (∗: Notional)

	2012 Actual	2013 Estimate	2014 Request	2015∗	2016∗	2017∗	2018∗
Agency IT Services	158.5	-	168.4	168.4	168.4	168.4	168.4
- IT Management	14.6	-	17.6	17.6	17.6	17.6	17.6
- Applications	68.7	-	56.0	56.0	56.0	56.0	56.0
- Infrastructure	76.0	-	94.8	94.8	94.8	94.8	94.8

Table 6: NASA IT detailed budget 2012 – 2018 (million dollars) (∗: Notional)

References

Badger, L., Grance, T., Patt-Corner, R. & Voas, J. (2012). Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146.

Bisciglia, C. (2007). Let a Thousand servers bloom – Google official post. Retrieved September 2, 2014, from http://googleblog.blogspot.com/2007/10/let-thousand-servers-bloom.html

IBM/Google Academic Cloud Computing Initiative (ACCI). (2013). Retrieved September 2, 2014, from http://www.cloudbook.net/directories/research-clouds/ibm-google-academic-cloud-computing-initiative

Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regards to the protection of personal data and on the free movement of such data (General Data Protection Regulation); COM(2012) 11 final. (2012). Retrieved September 3, 2014, from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//EN&language=EN

Jansen, W. & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing*. Gaithersburg, MD, United States: National Institute of Standards and Technology (NIST) Special Publication 800-144.

Kundra, V. (2010). 25 Points Implementation Plan to Reform Federal Information Technology Management. Retrieved September 2, 2014, from https://cio.gov/documents25-point-implementation-plan-to-reform-federal-itpdf/

Mell, P. & Grance, T. (2011, September). The NIST Definition of Cloud Computing. Gaithersburg, MD: National Institute of Standards and Technology (NIST) Special Publication 800-145.

FY 2013 Presidents Budget Request Summary. (2013). Retrieved September 2, 2014, from http://www.nasa.gov/sites/default/files/659660main_NASA_FY13_Budget_Estimates-508-rev.pdf

FY 2014 Presidents Budget Request Summary. (2014). Retrieved September 2, 2014, from http://www.nasa.gov/pdf/750614main_NASA_FY_2014_Budget_Estimates-508.pdf

NASA's Progress in Adopting Cloud-Computing Technologies. (2013).

Audit of GSA Transition from Lotus Notes to the Cloud. (2012). NASA Office of Inspector General.

Ross, R. S. (2013). Security and Privacy Controls in Federal Information Systems and Organizations. National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev.4.

Ross, R. S. & Johnson; L. A. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems. National Institute of Standards and Technology (NIST) Special Publication 800-37 Rev.1.

Spector, A. (2011). Academic Success in Cluster Computing. Retrieved September 2, 2014, from http://googleresearch.blogspot.com/2011/12/academic-successes-in-cluster-computing.html

Terdiman, D. (2009). White House unveils cloud computing initiative. Retrieved September 2, 2014, from http://www.cnet.com/news/white-house-unveils-cloud-computing-initiative/

FedRAMP Concept of Operations (CONOPS). (2012). Version 1.0.

Federal Risk and Authorization Management Program (FedRAMP) Security Controls. (2014a). Retrieved September 2, 2014, from http://www.gsa.gov/portal/category/102375

FedRAMP_Baseline_Security_Controls_01_06_2012_v1.0 - MS Excel spreadsheet file. (2014b). Retrieved from http://www.gsa.gov/portal/category/102375

Utin, M. (2015). From Misconceptions to Failure: Security and Privacy in US Cloud Computing FedRAMP Program. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 628–660. Retrieved October 25, 2015, from http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Utin, M. A. & Utin, D. (2012a). Cloud Computing: a new approach to securing personal information and addressing new EU regulations. Talk at DeepSec Nov. 2012, Vienna.

Utin, M. A. & Utin, D. (2012b). Private Information Protection in Cloud Computing – Laws, Compliance and Cloud Security Misconceptions. Talk at OWASP AppSec DC 2012, April, 2012.

Virka, B. (2013). Inspector General audit finds problems with NASA's cloud computing efforts. Retrieved September 2, 2014, from http://phys.org/news/2013-07-inspector-problems-nasa-cloud-efforts.html

Salesforce lands $28M GSA-wide cloud contract. (2011). Retrieved September 2, 2014, from http://washingtontechnology.com/Articles/2011/10/20/Salesforce-GSA-acumen-cloud-project.aspx?Page=2

Wikipedia. (2014a). Cloud computing — Wikipedia, The Free Encyclopedia. [Online; accessed 3-September-2014]. Retrieved from http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=623832473

Wikipedia. (2014b). Vivek Kundra — Wikipedia, The Free Encyclopedia. [Online; accessed 3-September-2014]. Retrieved from http://en.wikipedia.org/w/index.php?title=Vivek_Kundra&oldid=605452897

Wikipedia. (2014c). Wide area network — Wikipedia, The Free Encyclopedia. [Online; accessed 3-September-2014]. Retrieved from http://en.wikipedia.org/w/index.php?title=Wide_area_network&oldid=623860042