Secure Use of Cloud Computing in the Finance Sector

Good practices and recommendations

DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Rossen Naydenov, Dimitra Liveri, Lionel Dupre, Eftychia Chalvatzi

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

This work has been done in collaboration with Cloud Security Alliance, and in particular with the experts Marina Bregu, Daniele Catteddu, Dr. Jesus Luna and Damir Savanovic.

We would also like to thank the following people who helped in creating this report (in no particular order):

Gerasimos Moschonas, Group Information Security Officer, Alpha Bank, Greece

Jan Paredis, Citi, Belgium

Andrew Brian Sturman, Citi, UK

Fabien Huraux, Clearstream, EU

Frank Fischer, Deutsche Börse AG, EU

Tomislav Vazdar, CSO, Erste & Steiermärkische bank d.d., Croatia

Peter Debasse, KBC, Belgium

Christos Topakas, Piraeus Bank, Greece

Fabio Gianotti, Unicredit, Italy

Mario Maawad Marcos, Director of Fraud Prevention at Caixabank – Chair of the Financial Working Group at CSA, Spain

Roberto Baratta Martinez, Abanca, Spain

Stephanos Chasiotis, Raiffeisen, Poland

Jim de Haas, ABN AMRO, Netherlands

Nathaly Rey, Google, UK

Mario Kozina, National Bank, Croatia

Terhi Wathén, Finanssivalvonta - Financial Supervisory Authority, Finland

Heli Mäkitalo, Finanssivalvonta - Financial Supervisory Authority, Finland

Cécile Gellenoncourt, Commission de Surveillance du Secteur Financier, Luxembourg

Miranda Chilvers, Supervisor Operational Risk, De Nederlandsche Bank

Evert Koning, Head of Department Operational Risk and Data Quality, De Nederlandsche Bank

Gino Thielemans, Head of IT Supervision, National Bank of Belgium

Finally we thank the experts of ENISA Expert Group in Finance, the members of the Task Force for IT Supervision and European Banking Authority (EBA) as well as all participants to the validation workshops held in London on October 14th 2015 in providing us useful feedback during discussions.

ISBN 978-92-9204-138-0, DOI 10.2824/199301

Table of Contents

Executive Summary

Cloud computing is gradually being adopted within the European financial industry. However, the adoption approach is not yet mature. The vast majority of Financial Institutions (FIs) still rely on in-house infrastructure.

Finance sector Institutions and supervisory authorities seem to have a clear view of the financial and technical benefits connected to the adoption of both Public and Private Cloud[1] deployment models, but they remain cautious about the risk of losing control over information assets.

The most common approach used by FIs is a Hybrid of Private and Public Cloud. Even then, the services most often migrated to the cloud are test environments and email management[2]. Financial Institutions consider that Private Cloud is a better overall fit for the financial market due to privacy and compliance concerns. Private Cloud is certainly favoured by the National Financial Supervisory Authorities (NFSAs), as it provides more control over data and operations.

In creating this report we analysed input from a number of different sources to better understand the usage of cloud services in the finance sector. Based on the analysis we provide recommendations to financial institutions, regulators and cloud service providers about what we believe should be done to support secure adoption of cloud services in the finance sector.

As with business sectors even less critical than the finance sector, loss of control and compliance top the FIs' and regulators' list of risks. Whether the risk is perceived or real, this certainly poses challenges for the cloud market players to address. Those challenges include the ability to:

- Manage the governance and compliance risk
- Provide better tools for contract/SLAs negotiation (especially for smaller financial institutions)
- Increase the level of transparency of the Cloud Service Providers (CSPs)
- Increase the information understanding of cloud security in NFSAs and FIs
- Clarify the differences between outsourcing and cloud computing
- Push the NFSAs to provide more guidance on cloud adoption
- Improve currently available security and privacy certification schemes

From the information collected through the surveys and interviews, it appears that the most pressing short-term issues for promoting the adoption of cloud services are:

- **Reducing the information gap.** Neither FIs nor NFSAs consider security as a main benefit of cloud services, despite the fact that security is considered a very important factor by CSPs, and by expert bodies including ENISA, which has published reports (e.g., the ENISA Cloud Risk Assessment) describing the security benefits of cloud computing. Furthermore, in many instances regulators do not differentiate between outsourcing and cloud computing.

1 Good Practice Guide for securely deploying Governmental Clouds, ENISA (2013) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/good-practice-guide-for-securely-deploying-governmental-clouds
2 "Cloud computing - statistics on the use by enterprises", Eurostat (2014) http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

- **Providing clearer and fit for purpose regulatory guidance.** That CSPs, FIs and NFSAs have such different views and understandings of the relevance of national regulations for the cloud computing seems to confirm that the financial market needs better guidance and communication between the players.
- **Simplifying and streamlining compliance.** Further guidance from NFSAs would facilitate the adoption of cloud services in the finance sector while meeting the regulatory requirements. Various FIs find ENISA's Cloud Computing Security Risk Assessment[3] as a helpful tool for developing a corporate risk assessment for cloud computing.

In the longer term, some NFSAs fear a systemic failure stemming from the use of cloud computing by pan-European banking groups in connection to global cloud providers that offer services to multiple financial institutions. Such a risk of failure calls for stronger coordination and collaboration between NFSAs, and a more open dialogue with FIs and CSPs.

In terms of mitigating actions, while FIs are relying on SOC 2, ISO/IEC 27001, PCI DSS, some are also leveraging ENISA's cloud computing security risk assessment, which helps them identify key risks associated with Cloud and what actions to take.

CSPs report that for FIs, sometimes the biggest obstacle to cloud adoption is misconceptions about the technology. In fact, many EU NFSAs tend to block cloud usage, since they judge that CSPs are not sufficiently transparent. Therefore, it encourages CSPs to strive for transparency and help customers understanding the security implications of various cloud offerings.

In this study we provide the following recommendations:

- NFSAs, FIs and CSPs to cooperate on extending the national good practices and standards in the areas of Cloud governance and risk management
- NFSAs to define practices and standards for incident information sharing
- NFSAs to define minimum security requirements for adoption of Cloud computing in FIs
- FIs to develop a Cloud strategy in order to define their approach to Cloud computing
- CSPs to continue their efforts to provide transparency and assurance to NFSAs and FIs
- EU institutions in cooperation with CSPs to create information campaigns to better inform both regulators and FIs about the security risks and opportunities connected to the use of cloud computing
- EU institutions in cooperation with NFSAs to continue their work on harmonizing the legal and regulatory environment within the European Union

This study presents not just challenges and issues, but also some significant success stories that will be of good guidance and an example for those FIs, supervisory authorities and CSPs that are still at the beginning of their journey towards cloud. One conclusion we can derive from our surveys and analysis is that whenever the rules of the game are clear, more players are encouraged to participate.

Lastly, most of the issues highlighted in this report represent from our standpoint an opportunity for CSPs and technology providers to strengthen their offerings in order to enable financial institutions to better leverage the benefits of cloud computing.

3 "Cloud Computing Risk Assessment", ENISA (2009) https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

1. Introduction

Financial Institutions, such as banks, insurance companies and other financial service providers had an initially cautious approach towards cloud computing. This is mainly due to the many compliance and reputational risks, that such a new approach to IT service provisioning could entail. Nevertheless, in the recent years driven by the compelling business and economic benefits, FIs have been rapidly rolling out their cloud strategies. Currently, it appears that very few FIs still have a strict "no cloud" policy.

1.1 Policy Context

Cloud computing drives the vast spectrum of current and emerging applications, digital products and services. It is also a key technology enabler for the future Internet. Its direct economic value to the European Union is unambiguously significant. Cloud computing is an accepted enabler for innovation and also widely advocated as such by the European Commission (EC) in the Digital Single Market[4] which considers cloud computing an economic game changer. It also considers that the main obstacles impeding cloud adoption are standards, certification, data protection, interoperability, lock-in, and legal certainty[5].

The European Cloud Computing Strategy, contains the key actions that the European Commission identified to support the uptake of Cloud computing in Europe.

The European Cloud Computing Strategy has two main objectives:

- To make Europe cloud-friendly and cloud-active
- To connect digital agenda initiatives

Achieving these two objectives requires the execution of three key actions:

- Standards and certification
- Fair Service Level Agreements (SLAs)
- A European Cloud Partnership

As identified in the ENISA study *Network and Information Security in the Finance Sector*[6], information security measures are dispersed across many European and National regulations. Such fragmentation increases the need for common and shared guidelines as companies operate more and more at the pan-European level.

Trust and security in the digital world are the very foundations of a Digital Single Market (DSM)[7]. The DSM strategy aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy. The European Commission has identified the completion of the DSM as

4 "A Digital Single Market Strategy for Europe" COM(2015)192, European Commission, (2015) http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf
5 http://ec.europa.eu/priorities/docs/pg_en.pdf.
6 Network and Information Security in the Finance Sector. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector. (2015).
7 http://ec.europa.eu/digital-agenda/en/digital-single-market.

one of its top priorities[8]. The 2013 European Commission proposal for a Network and Information Security (NIS) Directive [9] aims to ensure a high, common level of cybersecurity in the EU, by:

- Improving Member States' national cybersecurity capabilities
- Improving cooperation between Member States, and between public and private sectors
- Requiring companies in critical sectors – such as energy, transport, finance and health – as well as key Internet services to adopt risk management practices and report major incidents to the national authorities

Another important initiative from the European Commission is the Capital Markets Union [10](CMU). With the CMU, the Commission will explore ways of reducing fragmentation in financial markets, diversifying financing sources, strengthening cross border capital flows and improving access to finance for businesses, particularly SMEs. The CMU is a new frontier of Europe's single market and is included in the political guidelines announced[11] by the Juncker Commission.

Finally, there is a large body of related work on the security and governance aspects of cloud computing, including ENISA work related to this analysis:

- *Cloud Computing: Benefits, Risks and Recommendations for Information Security*[12], which covers the evaluation of security risks of migrating to the cloud, legal considerations and the ENISA Cloud Computing Information Assurance Framework[13]
- *Security and Resilience in Governmental Clouds*[14], which provides a guide for public bodies in the definition of their security and resilience requirements, and how to evaluate and choose from the different cloud computing service delivery models
- ENISA's survey of current practice in public procurement[15], which covers over 140 public organisations across Europe
- *Procure Secure*[16], a guide to monitoring of security service levels in cloud contracts
- *Critical Cloud Computing*[17], a Critical Information Infrastructure Protection (CIIP) perspective on cloud computing services

8 http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.
9 "Concerning measures to ensure a high common level of network and information security across the Union" COM(2013)48, European Commission (2013) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666
10 http://ec.europa.eu/finance/capital-markets-union/index_en.htm
11 http://ec.europa.eu/priorities/docs/pg_en.pdf.
12 Cloud Computing: Benefits, Risks and Recommendations for Information Security. Online: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment. (2009)
13 ENISA Cloud Computing Information Assurance Framework. Online: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework. (2009)
14 ENISA. Security and Resilience in Governmental Clouds. Online: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/. (2011).
15 Survey and analysis of security parameters in cloud SLAs across the European public sector. Online: http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector. (2011).
16 Procure secure. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts. (2012).
17 Critical Cloud Computing. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing. (2013).

- *Incident Reporting for Cloud Computing*[18], which analyses how cloud providers, customers in critical sectors, and government authorities can set up cloud security incident reporting schemes
- *Network and Information Security in the Finance Sector*[19], which aims at understanding and comparing the obligations relevant to Information Security within the finance sector in most of the EU28 Member States, to compare them with the Industry's prospects, and to draw a clear vision of important priorities for the future
- *Security Framework for Governmental Clouds*[20], which gives guidance on the process from pre-procurement through finalisation and exit from a cloud contract, explaining the steps to take when focusing on security and privacy

1.2 Objectives and scope

The goal of this study is to highlight risks and opportunities, and to provide recommendations to the finance sector, with regards to the adoption of cloud computing services. In particular the objectives of the study are to:

- Provide an overview of the current level of maturity and adoption of cloud computing services in the European financial market
- Identify current regulations pertaining to Cloud Computing adoption in the finance sector
- Present a strategic approach to adoption of cloud-based services (Public Cloud, and Private Cloud both in-house on-premises and by external providers)
- Identify possible obstacles and facilitating factors to cloud adoption
- Understand the risks associated with cloud migrations, and how FIs mitigate them
- Provide an overview of the opportunities offered by cloud computing to the finance sector

This document focuses on cloud-related information security challenges and opportunities in the European Finance Sector.

The recommendations put forth are mainly addressed to FIs and regulators.

1.3 Target Audience

The results of this report targets the following audiences:

- Financial Institutions (FIs) such as banks trust companies, insurance companies and investment dealers
- National Financial Supervisory Authorities (NFSAs) who are in charge of financial institutions supervision
- Cloud Service providers (CSPs) and Cloud Brokers seeking for further guidance related to security approaches adopted by FIs, in order to identify and better understand specific needs and requirements that might be used to better tune their existing Cloud service offerings

18 Incident Reporting for Cloud Computing. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing. (2013).
19 Network and Information Security in the Finance Sector. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector. (2015).
20 ENISA. Security Framework for Governmental Clouds. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds. (2015).

1.4 Approach

In order to meet the objectives of this study, we have taken a methodological approach to report the analysis of desktop research, surveys and interviews.

The collection of data was based on:

- Desktop Research. This included sources such as: 1) studies and reports from relevant analysts, 2) blogs, web articles, white papers available on the Internet, 3) scientific publications, and 4) vendor-specific white papers (a complete list of references can be found in Annexes 1 and 4)
- Surveys and interviews. Two questionnaires were developed, one addressed to FIs and CSPs and another to NFSAs (see Annexes 2 and 3 respectively). In order to ensure the quality and plausibility of the surveys, the questions were reviewed by a selected group of individual representing the three categories to be surveyed. The questionnaires were used to survey a list of contacts including 83 representatives of FIs, 40 CSPs and 24 NFSAs. During the survey's phases, information was initially collected in written form and then, based on the participants' availability, discussed in a phone interview.
  A total of 42 organisations participated in the survey (24 FIs, 6 CSPs and 12 NFSAs), and a total of 24 interviews were conducted (13 with FIs, 1 CSP and 10 with NFSAs). We have tried to contact many more organizations from all parties (FIs, NFSA and CSPs) and from different member states. Due to time limitations only the ones that have responded to us, have been included in the survey and the interviews.

The information collected from research, surveys and interviews was consolidated and analysed to support developing the conclusions and recommendations. The content and structure of the designed surveys drove the analysis of the data collected.

1.5 Document structure

This document is organised as follows: Section 2 introduces the current state and approach of the financial industry to cloud computing, incentives and benefits, regulatory environment, risks and challenges and mitigation measures. It also contains the analysis of risks and opportunities from the perspective of different stakeholders. Section 3 details the relevant outcomes from the state of the art survey and desktop research, and also introduces the underlying roles and definitions to be used in this report. Section 4 summarizes the main conclusions and recommendations drawn from this report. Annexes 2 and 3 present the questionnaire used during the interviews with the selected representatives from FIs, NFSAs and CSPs.

2. Cloud adoption in the European Finance Sector

2.1 Current state and approach to cloud computing

The European financial industry is still in its early stages of cloud adoption. Many FIs use a limited range of cloud based services. Their approach using cloud based services is not strategically placed and in some cases they may be unaware that their services are cloud based.

As shown in Figure 1, almost 88% of FIs are already using cloud based services before June 2015, and 81% were aware these were cloud-based and their implications. In approximately 1 out of 4 organisations consulted, there were business units using cloud based services without the involvement of the respective IT department ("shadow IT").

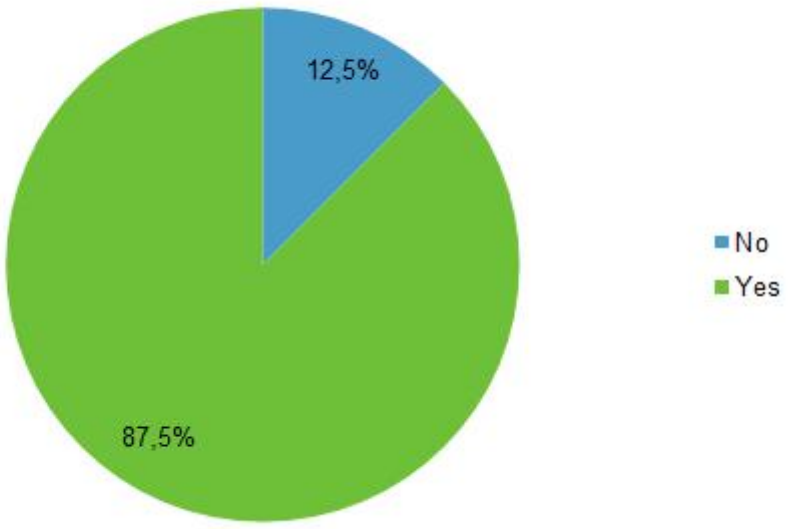

Figure 1 - Has the organisation you work for ever used cloud services?

Confirming the relatively low level of maturity of the adoption of cloud-based services by the finance sector, only 50% of finance sector involved in this study already have an explicit cloud strategy. The most common approaches use a hybrid of Private Cloud and Public Cloud (50%). Rather common (42%) is also the practice of relying on in-house IT and moving non-critical services (e.g., email management, collaboration and content management tools) to a cloud based service. Some organisations are using cloud based service as a testing environment and to develop use cases to better assess a hybrid of Public Cloud and in-house, on-premises hosting of cloud-based services. Public Cloud is also used by those FIs as test beds for new applications.

It must be stated that according to the results of our survey, a small percentage (8%) of FIs have chosen a strict Private Cloud only policy. The main reasons are privacy and compliance concerns, as well as the confidence that a Private Cloud can satisfy the business requirements of the organization. The vast majority (92%) of the organisations with an already developed strategy rely on a hybrid of Public and Private Cloud hosted both externally and also as in-house IT services. This is a sign of growing confidence towards the

adoption of cloud based services. However, we have noted a certain level of prudency when it comes to moving critical services to the cloud. Some are avoiding moving core banking activities to the cloud, instead opting to use it for the digital transformation of their business.

42% of FIs participating in this study either do not have an explicit cloud strategy or are just now in the early stages of developing one.

The main reasons[21] for FIs not having a well-defined cloud strategy are:

- **Regulation restrictions that prevent financial institutions from using the cloud (50%)**
- **Lack of strategic approach to cloud computing within the organisation (30%)**
- **Concerns over public breach notification (20%)**
- **Doubts about the real value of Cloud Computing (20%)**
- **Lack of interest - resources to assess the cloud opportunities (10%)**
- **Concerns over government surveillance (10%)**

Finally, around 8% of the FIs have a no-cloud strategy, i.e., either they will not adopt cloud based services or they have not yet had the time or resources to address this topic.

The main reasons[22] for FIs having a no-cloud approach are:

- **Security concerns (100%)**
- **Privacy concerns (100%)**
- **Legal/Regulatory/Supervision compliance (100%)**
- **Cloud providers do not comply with our internal policies (100%)**
- **We are waiting for a wider adoption from the industry (50%)**

The majority (60%) of the NFSAs declared to have a conservative or very conservative adoption of new technologies such as cloud. However, 40% considered themselves to be progressive or very progressive when referring to the adoption of cloud based services.

Almost half of NFSAs declared to have a level of knowledge of cloud computing that can be described as medium (27%) or poor (18%). It must also be pointed out that NFSAs declared similar levels of expertise with regard to information security (64% claim proficient/expert, but 36% have a medium or poor level of knowledge on the matter).

21 These are not cumulative to 100%, as participants could choose more than one reason in response to this survey question.
22 These are not cumulative to 100%, as participants could choose more than one reason in response to this survey question.

Finally, the low level of maturity within the Finance sector- with regards to the adoption of cloud based services- is evidenced by the answers provided by the NFSAs. The general perception of the NFSAs is that the level of adoption of cloud based services in the finance sector is low (64%) or very low (18%), and only 18% believe that the level of adoption is medium or high. This suggests that the NFSAs seem to be aware that cloud based services are still in the early stages of adoption within a Financial Institution. However, this underestimates the real level of cloud adoption.

Since security and privacy are considered as two of the main reasons preventing a wider adoption of cloud, it is clear that a better understanding within NFSAs about cloud based services, information security and the cyber security risks related to cloud adoption, would greatly help the market to mature and improve.

For example the experience of Cloud Service Providers (CSPs) is much closer to that of the FIs. In their opinion, only 1 out of 5 FIs are already using cloud based services. CSPs report that the FIs they interacted with have either developed a clear cloud strategy, or have developed one during the design phase of a cloud adoption project.

The top public cloud services/applications that are being adopted provide a snapshot of what organisations are leveraging from current cloud providers. As seen from Figure 2a, the services most often bought by FIs from public CSPs are (1) email management[23], (2) business management[24] and (3) application development/ test environment. From the NFSAs standpoint, the most appropriate services that FIs should buy from providers of Public cloud based services are instead (1) application development/ test environment, (2) business management and (3) email management. From CSP experience with the FIs, the most often used public cloud services are (1) application development/ test environment, (2) mobile security elements, and many others.

23 E-mail and spam management
24 Collaboration and content management platforms, CRM, HR, ERP, Marketing and Customer support/ticketing

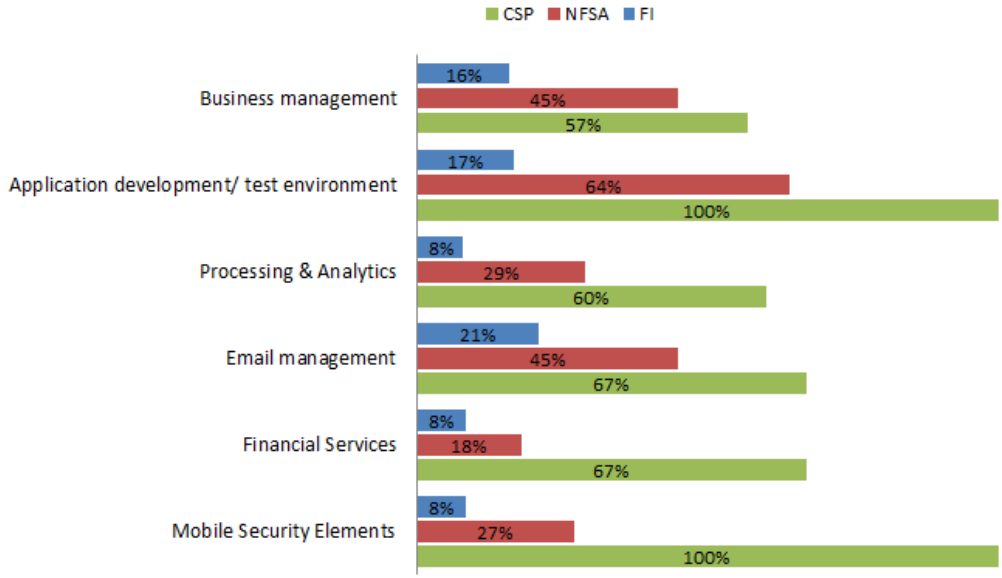

Figure 2a - Adoption of Public cloud based services

It is significant to note the inconsistencies between the opinions of FIs, CSPs and NFSAs with respect to which services should be bought from Public Clouds. While it is true that the three different groups have different priorities in mind, it is also true that email management and application development/test environment services rank very high in their assessments.

It should be noted that 23% of the participating NFSAs believe that Public cloud services should never be used in the finance sector.

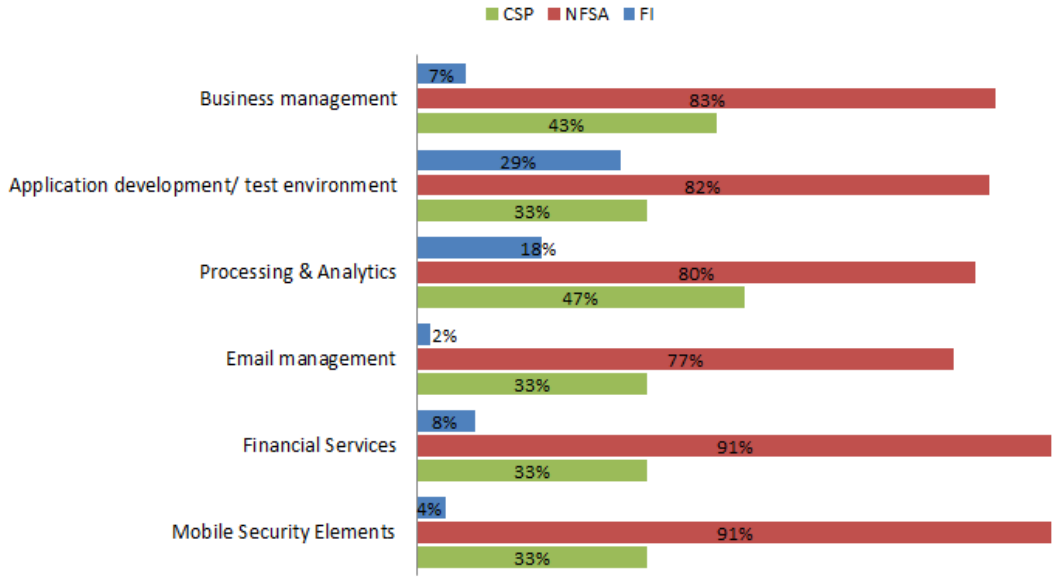

Figure 2b –Adoption of externally hosted, Private cloud based services

When it comes to the use of Private cloud based services (Figure 2b), it appears that FIs are mostly adopting (1) Application development/ test environment and (2) Processing & Analytics[25]. NFSAs believe that most Private cloud based services are appropriate, with (1) Financial services and (2) Mobile Security Elements being on top of the list. As seen from Figures 2a and 2b, NFSAs feel much more comfortable with the use of Private cloud over Public cloud. Again, CSP experience with FIs is that the Private cloud services that are used most often are (1) Processing & Analytics and (2) Business management.

By comparing the information depicted in Figure 2a and 2b, it is clear that while CSPs believe that Public cloud is fit for the FI's purpose, NFSAs for FIs are more in favour of using Private cloud. More neutral, and perhaps more informed and less biased, is the opinion of the FIs.

The messages that we can derive from the FIs' answers is that they prefer doing email management in a Public cloud rather than in a Private cloud, and that both Private and public clouds are suitable environments for application development and testing.

The strongest divergence between FIs, NFSAs and CSPs is related to the use of mobile security elements: from the viewpoint of the CSPs mobile security could be moved into the Public cloud, possibly to be offered a Security as a Service, while from the point of view of NFSAs those services should be provided from a Private cloud (possibly to guarantee scalability and keep full control as seen in Figure 2b). Finally from the point of view of FIs, mobile security elements are suitable for neither the Public nor the Private cloud.

2.2 Examples of cloud adoption in the Finance sector

In this section we provide several examples of how European supervisory authorities have been addressing some of the challenges from cloud based services, and how FIs are adopting cloud based services.

National Supervisory Authorities

DNB - The Dutch banking regulator

In 2012, De Nederlandsche Bank (DNB), the Netherlands' national banking regulator, was one of the initiators in Europe that enacted legislation allowing FIs to use cloud based services.

Now, DNB has included Amazon Web Services (AWS) for use by the country's finance sector, clarifying key supervision criteria (see "Guideline" below) for Dutch organisations looking to move infrastructure or services to the AWS cloud. The DNB's announcement means that Dutch banks and other FIs are if they comply to those guidelines now permitted to use AWS, Salesforce, IBM, KPN and Microsoft Azure[26] for a range of services including websites, mobile applications, retail banking platforms, high performance computing and credit risk analysis solutions.

The guidelines require that the DNB be allowed to oversee and confirm that the IT infrastructure (including cloud infrastructure) used by financial firms is compliant with its regulations. DNB confirmed that use of AWS Infrastructure as a Service (IaaS) meets this requirement. However, it has said that the FIs must still meet other requirements, such as carrying out a standard risk analysis for their use of IaaS cloud based services.

25 Processing capacity, data analysis and Intelligence, big data, storage/disaster recovery/data archiving, virtual desktops

26 http://www.globalbankingandfinance.com/dutch-regulator-de-nederlandsche-bank-makes-cloud-migration-a-seamless-reality/ .Last accessed 30th November 2015

The DNB guidelines require[27] institutions to:

- report their intention to use cloud computing to DNB beforehand
- draw up a risk analysis
- also meet the requirements laid down in the Financial Supervision Act (Wet op het financieel toezicht – Wft)
- allow DNB the right to examine the bank
- make sure exit clauses are included in the contract

FINMA - Swiss Banking Regulator

FINMA exercises prudential and risk-oriented supervision over banks and securities dealers. As a financial regulator it aims at protecting creditors and maintaining the stability of the financial system. Therefore, it centres on ensuring that licensing, as well as other legal and regulatory requirements, are met at all times. FINMA's level of supervision is most intensive in areas where risk is greatest. It assigns banks, insurance companies, collective investment schemes, self-regulatory organisations (SROs) and directly subordinated financial intermediaries (DSFIs) to six different supervisory categories depending on their size, complexity and risk structure.

When shortcomings arise and licensed institutions break the rules, FINMA orders appropriate measures to enforce supervisory law[28].

FINMA has allowed the use of cloud based services in Switzerland and the most prevalent are those offered by Safe Swiss Cloud. Safe Swiss Cloud claims to be a safe and secure cloud computing service based in Switzerland that offers innovative compute, storage and managed cloud services. They emphasize the privacy of customers[29] by committing to not share data with third parties, to fully comply with to Swiss[30] and EU laws[31] on data protection and data transfer.

Moreover FINMA adopts a risk-based approach[32] to asset management. There are six different supervisory categories to which licence holders are assigned, depending on their potential risk impact on creditors, investors, the system as a whole and the reputation of the Swiss financial centre. Licence holders of major and global systemic importance that are exposed to significant risks are assigned to Category 1. The risk potential of the institutions in the other categories decreases gradually down to Category 5. Market participants in Category 6 are not placed under prudential supervision since they are considered very low risk. Such an approach is also relevant to cloud computing.

27 DNB. (2015). Cloud computing: the rules. Available: http://www.dnb.nl/en/news/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-februari-2015/dnb319119.jsp. Last accessed 26th June 2015

28 FINMA. Available: https://www.finma.ch/en/supervision/our-approach-to-supervision/.

29 Safe Cloud Swiss. Available: https://www.safeswisscloud.ch/en/swiss-secure-compliant. Last accessed 11 September 2015

30 Swiss law: SR 235.1 Federal Act on Data Protection.

31 European Commission Decision 2000/518/EC (Official Journal L 215/1 of 25.8.2000).

32 FINMA. Available: https://www.finma.ch/en/supervision/institutions-and-products-subject-to-the-collective-investment-schemes-act/supervisory-approach/

Financial Institutions

Bankinter[33]
Bankinter is currently listed among the top ten banks in Spain. It has provided online banking services since 1996, when they pioneered the offering of real-time stock market operations. More than 60% of Bankinter transactions are performed through remote channels, and 46% of those transactions are conducted over the Internet.

Bankinter uses Amazon Web Services (AWS) as an integral part of their credit-risk simulation application, developing complex algorithms to simulate diverse scenarios in order to evaluate the financial health of Bankinter clients. According to the Bankinter Director of Technological Innovation, they perform at least 5,000,000 simulations to get realistic results. Bankinter uses the flexibility and power of Amazon Elastic Compute Cloud (EC2) to perform these simulations, subdividing processes through a grid of AWS EC2 instances, and implementing simulations in parallel on several AWS EC2 instances to obtain the result in a very short time period.

Through the use of AWS, Bankinter decreased the average time-to-solution from 23 hours to 20 minutes and dramatically reduced processing (and cost), with the capability to reduce even further when needed.

Bankinter reports that the AWS platform, with its unlimited and flexible computational power, is a good fit for their risk-simulation process requirements. They are empowered to decide how quickly to obtain simulation results. More importantly, they say that they have the ability to run simulations that were not before possible due to the large amount of infrastructure required[34].

ING
ING is using cloud-based software from ServiceNow to deliver HR services to its 25,000 staff in the Netherlands. ServiceNow and ING built a branded portal to give staff access to information and to automate previously manual tasks. ING previously used call centres and face-to-face interactions for most HR enquiries. Now a self-service portal gives employees faster and easier access to a knowledge base with over 1,200 articles on topics such as health and compensation. This improved user satisfaction and reduced the cost and time of providing services. ING sees ServiceNow as a key partner in their transformation efforts[35].

33 https://www.bankinter.com/www2/particulares/es/inicio/bienvenida
34 Amazon Web Services. AWS Case Study: Bankinter. Available: http://aws.amazon.com/solutions/case-studies/bankinter/.
35 ComputerWeekly.com. (2015). Dutch bank ING puts HR services in the cloud. Available: http://www.computerweekly.com/news/4500242949/Dutch-bank-ING-puts-HR-services-in-the-cloud.

2.3 Future adoption trends

The data collected on cloud based services already adopted by FIs, is consistent with the data related to cloud services that FIs would like to adopt in future (see figure 3a and 3b).

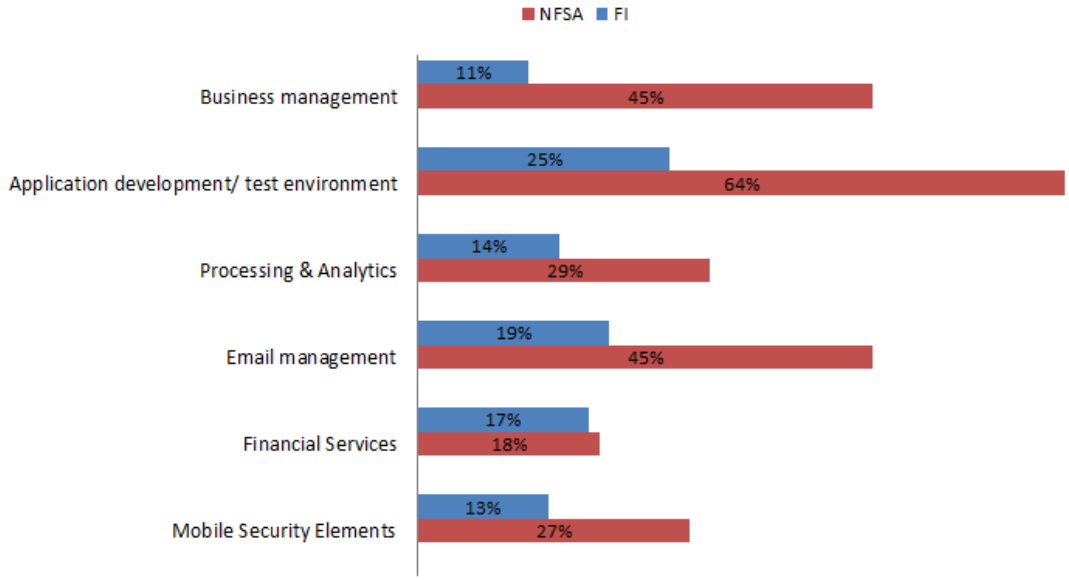

Figure 3a – Which Public cloud based services are you interested in adopting?

It appears that FIs do not see particular benefits in the use of Public cloud based services. The only use cases in which they see some value are application development/test environment (25%) and email management (19%). NFSAs appear to have similar opinions, as they believe that Public cloud is fit for application development/test environment (64%) as well as email management (45%) and business management (45%). It might come as a surprise that NFSAs seem to see more benefits in the use of Public cloud (e.g. for business management and e-mail management services) than the FIs themselves. FIs are somewhat open in using public cloud for collaboration and content management platforms (29%), and e-mail (29%), but beyond these services the interest in Public cloud based services is generally lower.

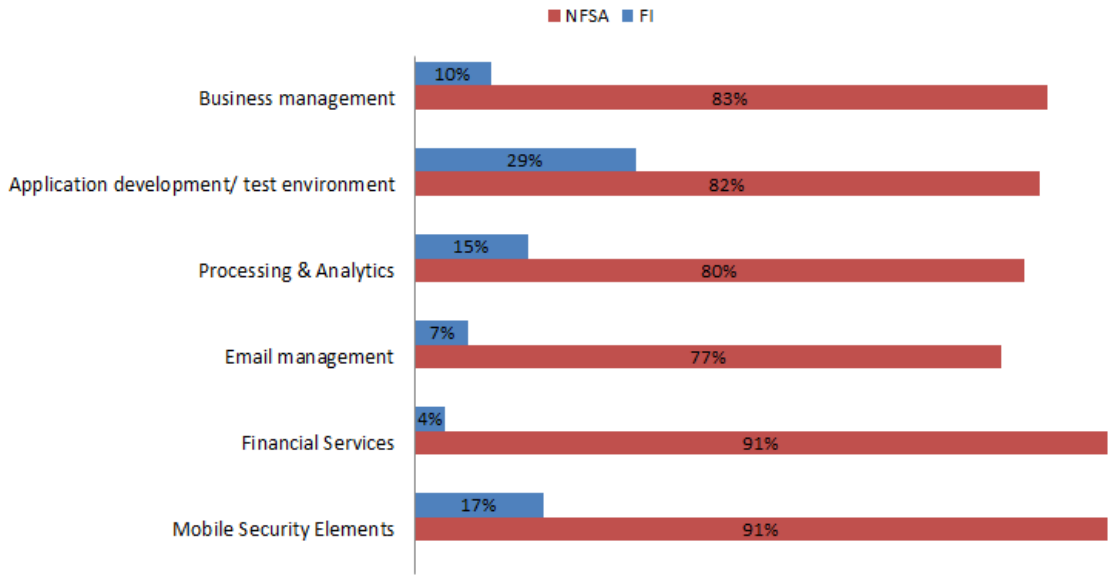

Figure 3b - Which Private cloud based services are you interested in adopting?

Similar to what we see in the Public cloud based services, FIs do not have high interest in adopting Private cloud based services, as the highest interest has been again noted in application development/test environment (29%) and while the interest in business management services is generally low, 38% of respondents were interested in collaboration and content management platforms. Based on the analysis of the data reported in Figure 3a and 3b, adjusted on the basis of the input collected during the interviews, we can state that both FIs and NFSAs see more benefits in the use of Private cloud rather than Public cloud. Moreover, most NFSAs strongly support and believe that Private cloud based services are mostly appropriate for use in finance sector, which represents an opportunity for growth in the cloud market.

In summary, by analysing the answers provided by FIs on their interest about Public and Private cloud, it is evident that FIs generally consider application development and testing as the best possible use cases for both Private and Public cloud. However, it is also noticeable that FIs perceive more benefits in the use of Public clouds for email management and financial services applications.

2.4 Incentives and Benefits

Our analysis shows that both financial institutions and supervisory authorities have a similar understanding of the benefits that the cloud based services are offering.

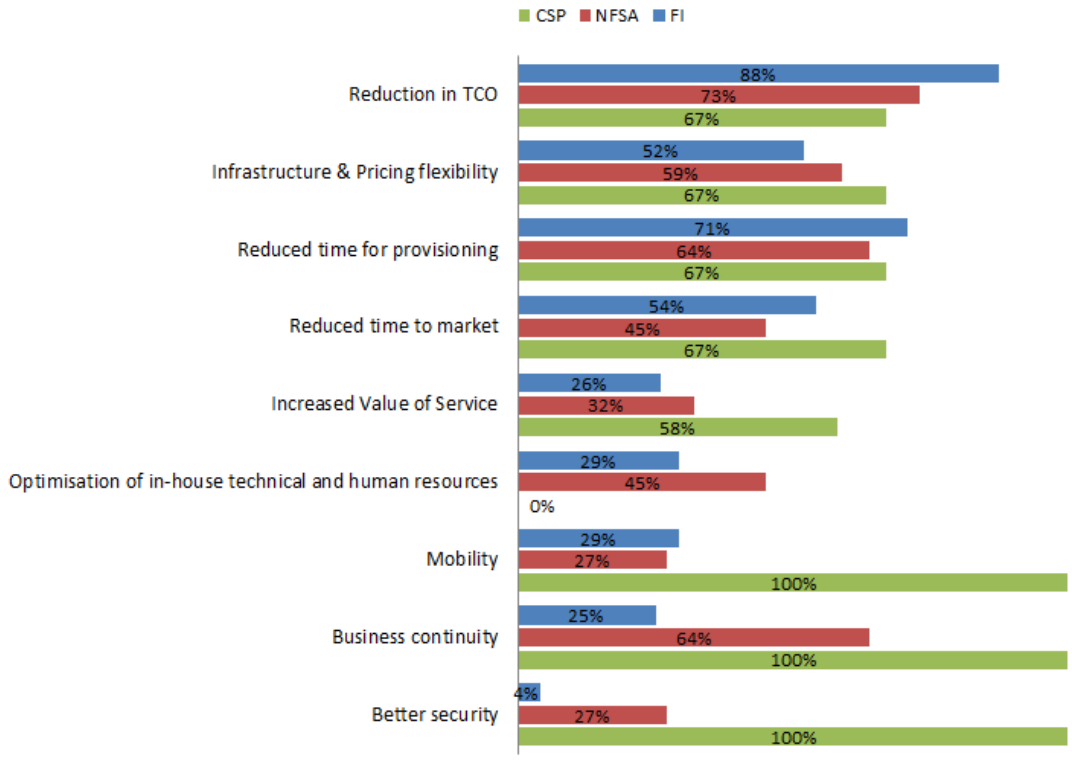

Figure 4 - Primary reasons for adopting cloud computing

Some of the top reasons to move to the Cloud (Figure 4) are reduced total cost of ownership (TCO), reduced time for provisioning, reduced time to market, and infrastructure and pricing flexibility. NFSAs also see business continuity as one of the important incentives for adopting cloud based services. On the other hand, NFSAs and almost 70% of the surveyed FIs do not consider mobility as an important reason for adopting the cloud, whereas CSPs believe it is, together with business continuity and security, the biggest reasons for the adoption of cloud computing services. However, CSPs do not believe that cloud computing can be leveraged by FIs for optimisation of in-house technical and human resources, which is a primary reason for 45% of the FIs.

It is worth highlighting that neither FIs nor NFSAs consider information security as one of main benefits and incentives for adopting cloud based services, although security is considered as very important factor from the CSPs perspective. This might be due to the fact that the security measures provided by the CSPs are not very well communicated to the NFSAs and the FIs. The opinion of the FIs and NFSAs seems to be in contradiction not only with that of the CSPs,

In general it appears that while both FIs and NFSAs are aware of benefits that cloud brings (specialization, economy of scale, flexibility), they are not willing to take the chance of losing over what is arguably the most valuable asset for a financial institution: the information.

but also with the perspective of other relevant experts (including ENISA) as stated in published reports (e.g. ENISA Cloud Risk Assessment[36]) regarding the security benefits of cloud based services. Some NFSAs say that better security is a benefit brought by cloud based services only for small FIs.

2.5 Regulatory Environment

Supervisory authorities around Europe are aware that an increasing number of FIs are adopting or considering the use of cloud based services. From the NFSA's perspective, it is important to understand the prudential statutory and subsidiary legislation relevant to cloud based services. In general, from the NFSAs' point of view, cloud based services are considered as a form of outsourcing and therefore the same rules apply to cloud based services as for outsourced services. Moreover, it appears that most of NFSAs are very cautious towards cloud base services, recommending the use of Private cloud over Public cloud, which they view as a suitable option only for non critical services.

Despite the fact that some NFSAs around Europe (e.g. the Netherlands, Spain, Greece, Finland) have published opinions related to outsourcing/cloud based services, it appears that the financial industry is dealing with a lack of clear, formal guidance that is consistent across all NFSAs on the specificities of cloud based services.

For instance, half of the participating NFSAs request that FIs notify them when adopting cloud services only if moving critical services or sensitive data (50%). However, this cannot be considered a general rule. Some NFSAs require to be notified always (33%), and just some of them when migrating to a Public cloud (8%).

Our respondents have described various cases in which the need to notify NFSAs about the adoption of cloud based services has caused severe delays, or even blocked the prospective use of cloud services in their FIs. This on one hand is because information was not provided by the CSPs, but on the other hand also due to lack of guidance from the NFSAs on what specific information to be provided.

A lack of formal guidelines for cloud based services, and the lack of mature evaluation processes, has forced the relevant NFSAs to perform evaluation that cause severe delays or even block the prospective use of cloud based services by FIs.

It appears reasonable to assume that those issues could have been mitigated by increasing the level of understanding of NFSAs about cloud based services and CSPs providing more specific information, which calls for better understanding, increased CSP transparency and a more structured and strategic approach from FIs and NFSAs. There is still a smaller group of NFSAs (8%) that have no specific requirements on the matter. However, however they do appreciate voluntary notification by the FIs.

About 70% of participating FIs indicate that they have engaged with regulatory bodies in discussions about requirements for the adoption of cloud based services in the finance sector. Several FIs are following specific regulations and standards to govern the migration to the cloud. These specific regulatory requirements are presented in Figure 5. The vast majority of the FIs need to comply with data protection legislations and other specific national regulations issued by individual NFSAs (e.g., IT service providers based in Luxembourg and offering IT operation services to a FI must obtain a license of finance sector professionals, also known as Support PSF to provide a secure and confidential processing of the data in Luxembourg). The Payment Card

[36] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

Industry Data Security Standard (PCI-DSS) is certainly another very important sector-specific standard with which the majority of the FIs must comply.

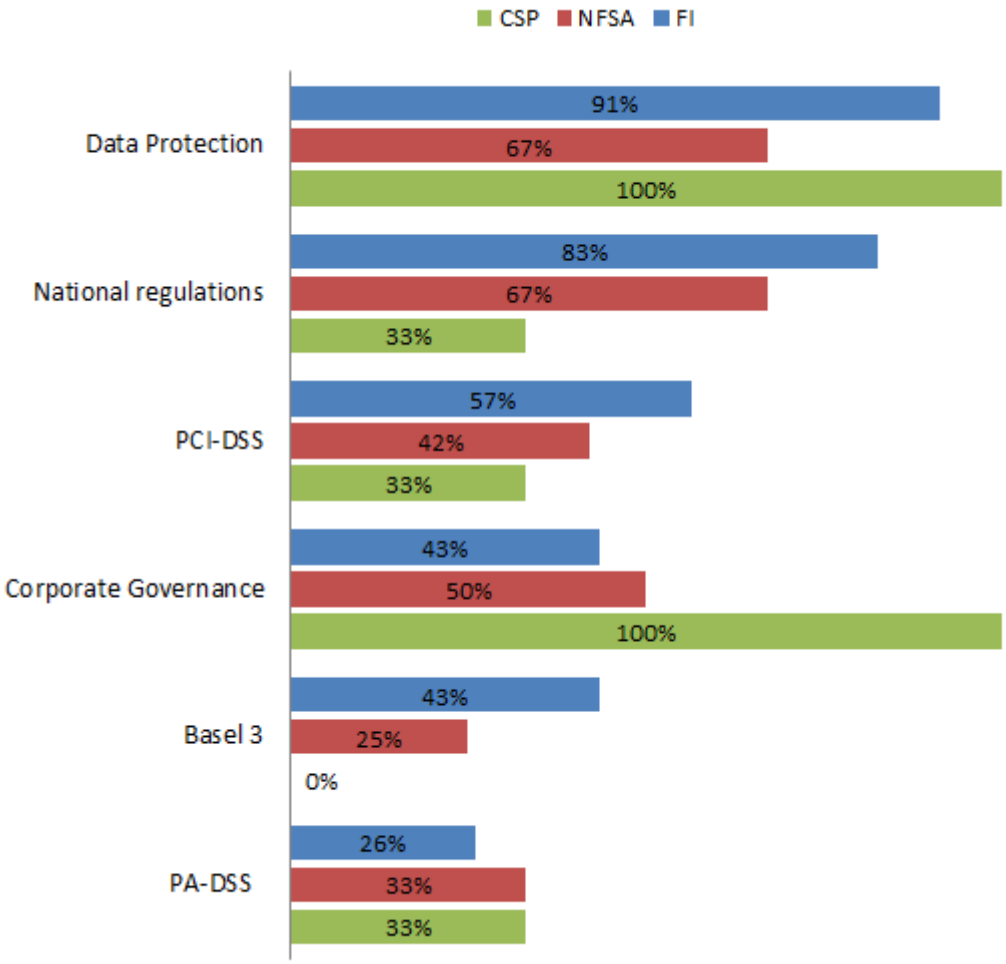

Figure 5 - Notable regulations - FI perspective

It appears that CSPs do not overly emphasise the importance of national regulations and PCI-DSS. Based on the experience they have in dealing with the FIs, the two most important regulatory requirements are data protection and corporate governance.

The fact that CSPs, FIs and NFSAs have such a different view and understanding of the relevance of national regulations for cloud based services seems to confirm that the finance sector is in the need of better guidance and better communication between the relevant players.

It should be noted however that even if there is still work to be done from the NFSAs' side, some virtuous examples already exists, for instance the DNB in the Netherlands. The Dutch Authority has provided formal guidance that states[37]:

> "When using third-party cloud computing services, the supervised institution is subject to the legal requirements that apply to outsourcing:

37 http://www.toezicht.dnb.nl/en/binaries/51-224828.pdf

- Risks must be demonstrably known and mitigated, and
- Outsourcing to third parties may not obstruct supervision.

Before a supervised institution proceeds to engage in cloud computing, DNB expects to be informed of this prospective outsourcing arrangement. DNB will ask the supervised institution to submit its risk analysis concerning cloud computing for assessment in the context of risk-based supervision."

Furthermore, DNB requests that explicit attention is given to risks associated with, among other things, data integrity, confidentiality and availability. DNB also requires assurance with regards to the location where the business data are to be processed and stored. In the event that the supervised institution interrupts the use of third party services, it must secure all data and verify that they have been removed from the third party's systems. The DNB has also defined the requirements for cloud computing risk assessment. Banks are required to prepare a risk assessment using a risk analysis framework[38] and contractually agree to a 'right to examine.' The ENISA Cloud Computing Security Risk Assessment is one that is known to have been used among others as well. The requirements set out in the Dutch Financial Supervision Act (Wft) also have to be met.

DNB has agreed to a 'right to examine' with various parties, including KPN, Microsoft, IBM, Amazon Web Services (AWS) and Salesforce.com. This 'right to examine' (right to audit) is a standard clause in the contracts that Dutch financial institutions use for cloud services provided by these CSPs. This allows financial institutions to meet one of the statutory requirements for cloud services.

In Germany, BaFin requires FIs to maintain full audit rights for its external and internal auditors. The same requirement applies for BaFin too when outsourcing to a provider. Any CSPs that are not willing to grant these rights cannot serve the German banks.

Bank of England requires FIs to make available on request to the Prudential Regulation Authority (PRA), as well as to any other relevant competent authority, all information necessary to enable competent authority to supervise the compliance of the performance of the outsourced activities with the requirements of the regulatory system.[39]

An area where there is consistency in the approaches of the various NFSAs is risk assessment and management. All the NFSAs require FIs to provide evidence that the information security risks connected to the use of cloud based services are properly identified, assessed, treated and communicated.

For instance, BaFin [40]requires that, in accordance with the German Banking Act (KWG) and the Minimum Requirements for Risk Management (MaRisk), FIs ensure the integrity, availability, authenticity and confidentiality of data within their IT systems and IT processes. In recent years, BaFin has increased its efforts in the area of IT security. Special audits have helped to raise awareness about IT security amongst the FIs.

38 http://www.toezicht.dnb.nl/binaries/50-228202.pdf
39 http://www.prarulebook.co.uk/rulebook/Content/Part/214147/11-09-2015
40 http://www.bafin.de/SharedDocs/Veroeffen-tlichungen/EN/Fachartikel/2013/fa_bj_2013_11_it_sicherheit_en.html

Banking supervision in Germany covers all risks related to the IT management/control, availability, confidentiality, integrity and authenticity of the data, internal control system of the IT organisation, IT strategy, and the use of information technology. BaFin has noted the challenge to maintain IT security at a high level when the framework conditions change. As many FIs have outsourced their IT, BaFin believes that it is crucial for them to integrate the service provider in their information security management functions/systems, since the same requirements apply irrespective of whether the IT systems and processes are managed by the FIs themselves or by service providers.

Financial institutions in Luxembourg are required to have a minimum internal IT capacity, which is proportionate to their business and system complexity. [41]

CSSF in Luxembourg requires FIs to follow at least three prudential principles:

- **The financial institutions shall always have their activities under control from a technical and operational perspective;**
- **The risks shall be correctly assessed, reduced, transferred or accepted;**
- **The residual risks shall be known and accepted.**

Bank of Italy[42] (BOI) requires FIs to choose CSPs on the basis of an analysis of the risk, which should include an estimate of:

- **The risks connected to the resources and services to be outsourced**
- **The risks attaching to possible suppliers**
- **The quality of sub-contractors**
- **The redundancy of the lines of communication used**
- **The reliability, security and scalability of the technologies adopted**

BOI also requires FIs to know the location of data centres and the number of staff that have access to confidential data or critical components, with the outsourcer obliged to update the data periodically.

Finally, BOI warn FIs to be especially cautious in evaluating CSP offerings. The regulator believes that in the case of acquisition of community or public cloud services, the potential risks are greater and may require a more complex system of controls, especially when critical components are outsourced. It is important that the locations of the data centres be notified in advance, and adequate mechanisms must be provided for isolating each client's data to protect their confidentiality and integrity. CSPs must contractually guarantee to comply with the agreed levels of service, including in emergencies or when other clients call for resources. CSPs should also ensure that data access and modifications can be fully reconstructed, including for inspections. According to BOI, FIs must agree on adequate audit procedures with the CSP.

41 http://www.cssf.lu/filead-min/files/Publications/Rapports_annuels/Rapport_2011/RA2011_chapter_10_eng.pdf
42 http://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c263/263CIRC_15AGG.pdf

NFSAs have noted that CSPs are proactively working to improve the level of transparency, but they still note differences between the approach that different CSPs have, and their ability to provide the sufficient level of transparency. As NFSAs require access to sufficient information to be able to understand risk exposure of FIs, there is an increased tendency to use a certification scheme for CSPs as a starting point for achieving compliance.

Finally, as banking groups with a global or pan-European presence have started using cloud computing, NFSAs started to consider cloud services as systemic services, and to be concerned with concentration of risk. Therefore, while some NFSAs have no interest to regulate the CSPs directly, some of them have expressed the potential need to oversee providers who are offering critical services to banks with a global presence, as they represent a source of systemic risk.

3. Risks and Challenges

3.1 Security concerns

The study shows a continued concern over security issues related to cloud. NFSAs unanimously agree that risks related to in-house IT can be much easier controlled and operationally managed than in the Cloud. With security concerns being a key consideration when adopting cloud services, we asked respondents to rank a list of common security risks on scale of one to five (with five being the greatest concern).

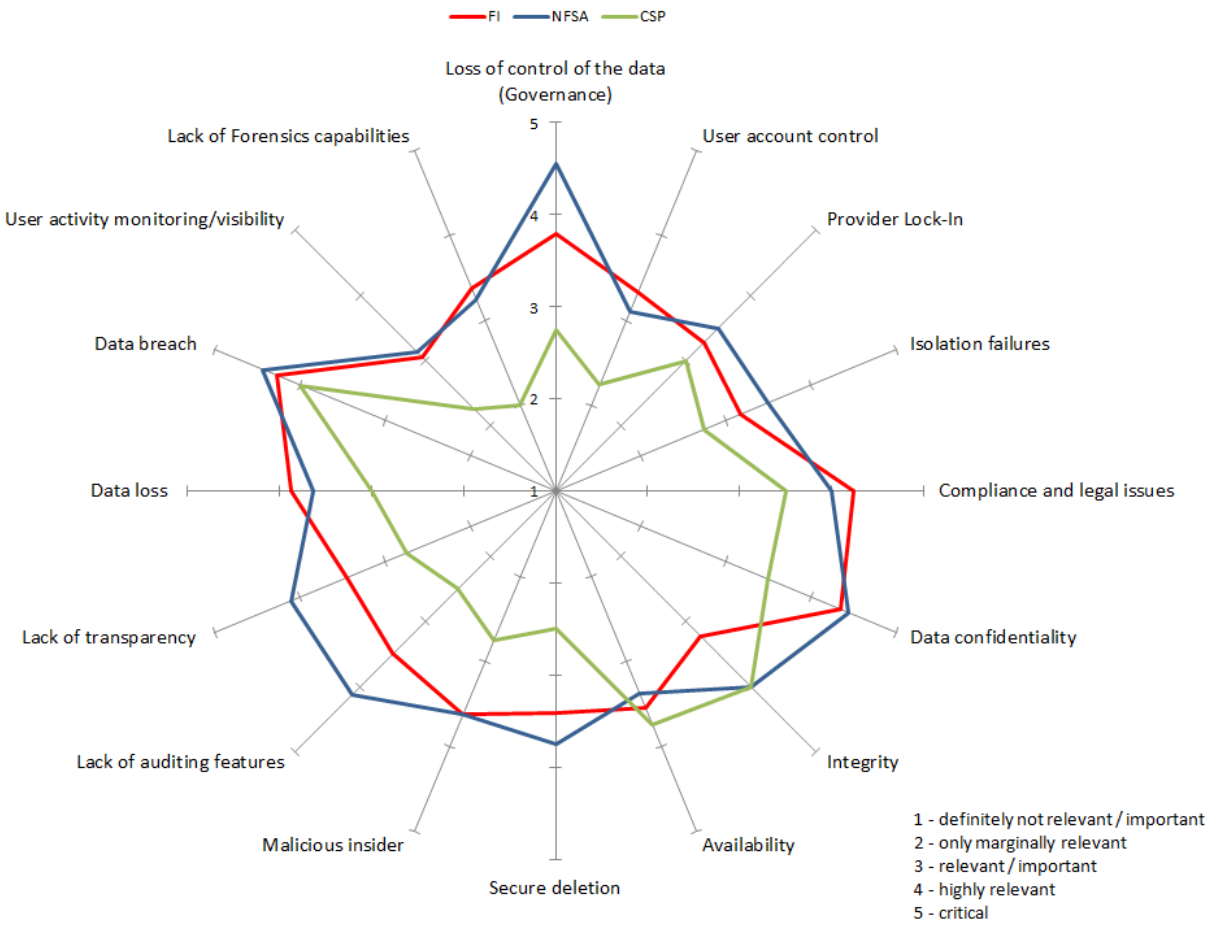

Figure 6 - Cloud computing security concerns ranked

The FIs have many security concerns related to cloud based services, but they are especially worried about data confidentiality, data breach, and compliance and legal issues. The NFSAs however perceive loss of governance, lack of transparency and lack of auditing features as additional top risks, in addition to those mentioned by FIs.

CSPs report that when they discuss security concerns with FIs, usually data breach, integrity and availability are top the list. It is worth noticing that lack of forensic capabilities is not considered as a particularly relevant issue, and generally all other risks are substantially less relevant than those expressed by FIs and NFSAs.

Similarly to other economic sectors[43], security concerns are considered the main limiting factor for cloud adoption in the finance sector (see Section 3.1). Analysing the answers provided to risk-related questions, it appears that NFSAs are generally more concerned than FIs. The biggest differences in perception noted are loss of control of the data (governance), integrity, lack of transparency and lack of auditing features.

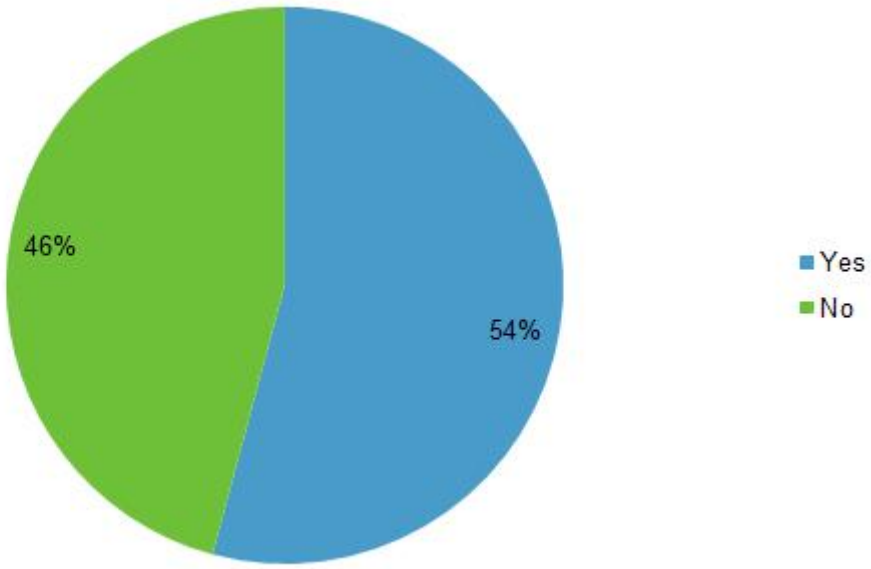

Figure 7 - Have you or your team developed a detailed corporate risk assessment of Cloud Computing?

3.2 Corporate Risk Assessment

Despite the fact that FIs seem to be aware of specific risks connected to the use of cloud computing and that NFSAs are requiring that supervised institutions to identify, assess and mitigate the risks, 46% of the respondents have not developed a detailed corporate risk assessment for cloud computing.

Such high percentage of FIs without a developed corporate risk management strategy for cloud computing is not surprising considering that, as noted in Section 3.1, 42% of the FIs do not have a fully structured cloud strategy.

The lack of clear and formal regulatory guidance could be another explanation of the fact that despite 88% of FIs having already used cloud services, 46% have not developed a detailed corporate risk assessment.

43 http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

From our standpoint, some further guidance from NFSAs could improve the situation and facilitate the adoption of cloud services in the finance sector while meeting the regulatory requirements. Various FIs find ENISA Cloud Computing Security Risk Assessment as a helpful tool on the market for developing a corporate risk assessment for cloud based services. Additionally, some of the respondents have identified Technology Risk Management Guidelines[44] issued by the Monetary Authority of Singapore as very useful to better guide for addressing existing and emerging technology risks.

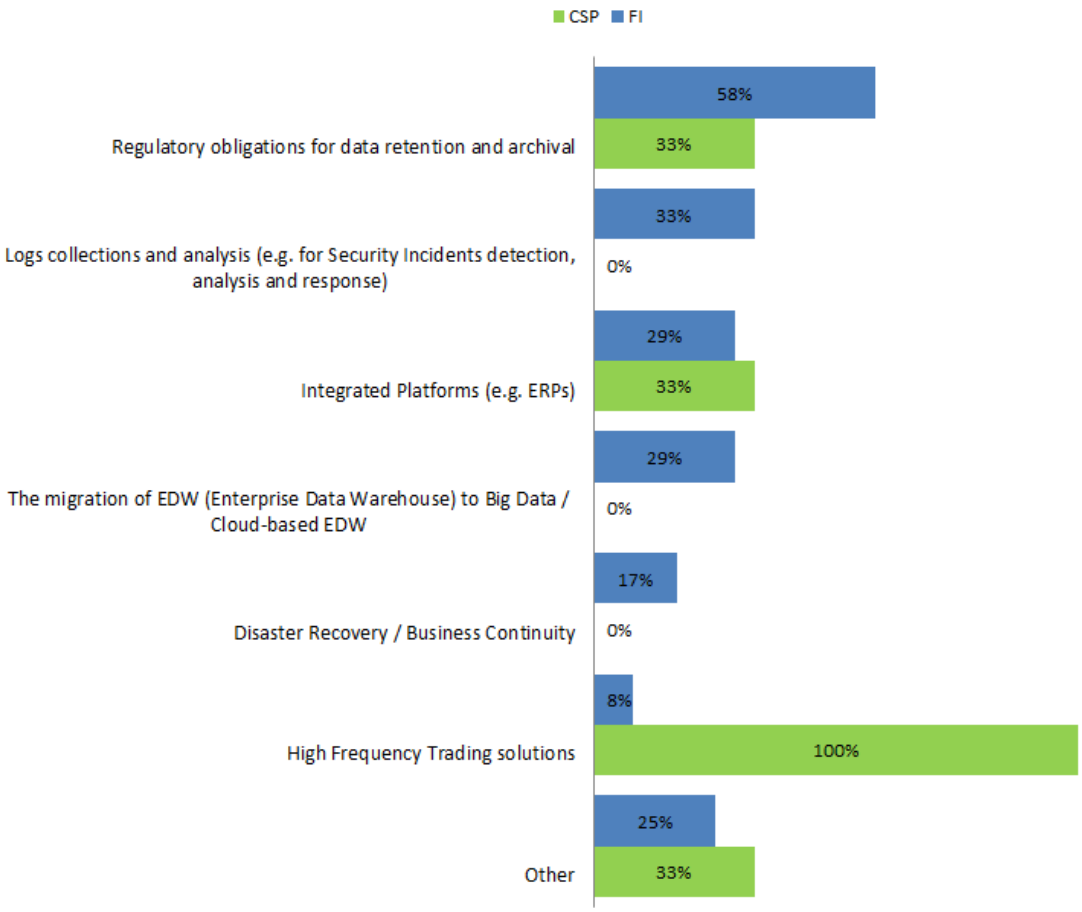

Figure 8 - Main challenges to cloud based services

Finally we asked CSPs and FIs which are the main challenges to their adoption of cloud based services. Their opinions from these interested parties are divergent. In fact from the FIs standpoint, regulatory obligations represent by far the biggest challenge during the migration to cloud-based services. For the CSPs however, the most complex challenge relates to the migration of high frequency trading solutions. In contrast, high frequency trading solutions are not seen as a challenge to FIs, perhaps because they are not planning to move these applications in the cloud. We believe it is important to note that while a third of the FIs recognise that log collection and analysis in cloud is an issue,

44 http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx

particularly in Public Clouds, the CSPs do not share the same opinion and they appear to judge the challenge of log collection as completely irrelevant. These divergent opinions seem to reflect the need of FIs to be in direct control of what happens in the cloud (and logs are a good tool for that).

4. Security requirements and mitigation measures

In this section we provide an analysis of the security requirements both from the point of view of FIs and CSPs. We report and analyse the security measures that NFSAs, FIs and CSPs would like to adopt within the finance sector.

4.1 Security requirements

When adopting (or planning) cloud services, financial institutions are strictly requiring:

- Thoroughly implemented security measures (75%)
- Deep auditing permission in case of incident (63%)
- Penalty clauses in case of incident (54%)
- Not moving client data to the cloud (50%)

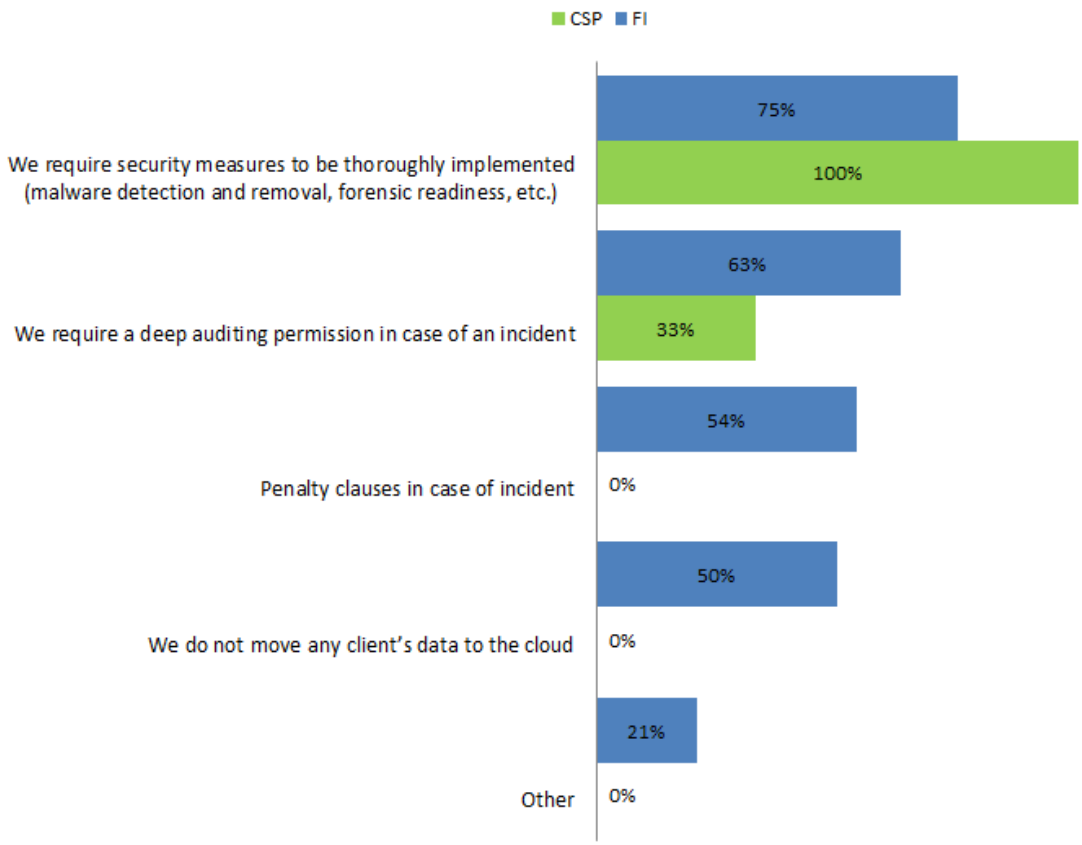

Figure 9 - Security requirements

CSPs mostly confirm that FIs ask for thoroughly implemented security measures, deep auditing permission in case of incident, and not moving client data to the cloud. However, it appears that penalty clauses in case of incidents are not required from FIs.

Isolating answers from smaller CSPs from those of leading European providers, it appears that FIs demand more from small CSPs, from whom they usually require deep auditing permission in case of an incident. Moreover, FIs do not move client data into clouds of smaller providers. FIs also seem more able to enforce penalty clauses in case of incidents to small CSPs, which is not the case with big providers. However it should be noted that we cannot consider this statistically significant since the sample of CSPs used was too small.

In previous sections we have already noted that many NFSAs still have concerns about the adoption of cloud based services by FIs. Those concerns are reflected by the fact that NFSAs require FIs to follow strict security requirements, starting with a risk assessment of security measures that need to be implemented.

Due to those stringent requirements and supervision by NFSAs, compliance is a crucial operating requirement for FIs, and cloud adoption must be considered within the context of maintaining regulatory compliance. This study found that organisations typically approach compliance assurance with cloud providers through these means:

- Specific contract clauses (92%)
- SLAs (83%)
- Certification (71%)
- Audits (29%)

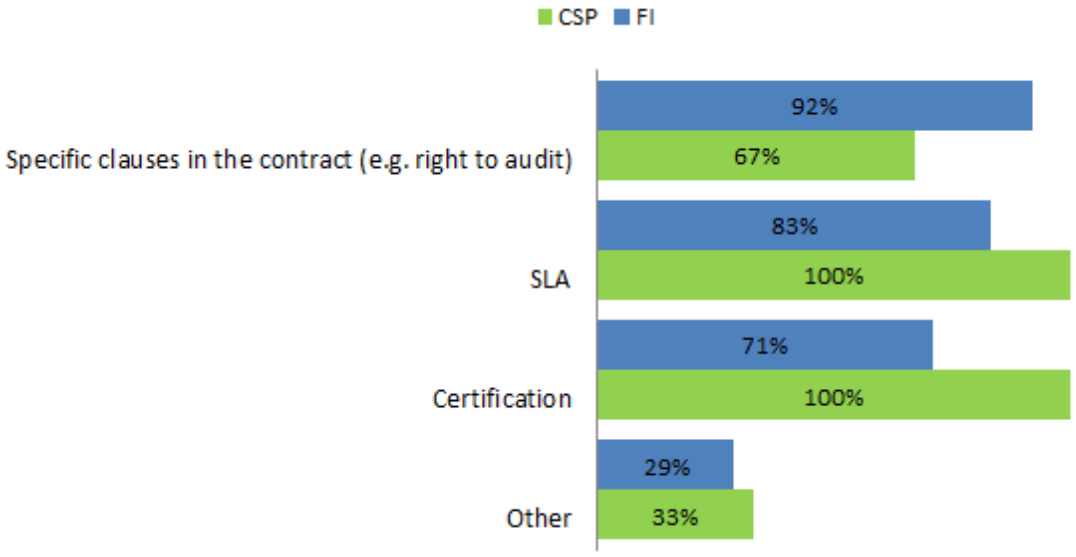

Figure 10 - Ensuring compliance by service providers

During the interviews we identified two challenges for FIs in their compliance efforts:

- **Lack of negotiation power.** FIs do not have enough power when negotiating specific contract clauses with large CSPs.
- **Perceived limitation in the area of certification.** While FIs see high value in attestation, e.g. SOC 2, or audits performed by NFSAs, there are mixed feelings about certification of cloud services. On one hand, there is consensus that certifications provide high value and are a good means for CSPs to assure their compliance with standards. On the other hand, it appears that financial market players are sceptical towards existing cloud certification schemes, especially due to lack of information about the relevance

of existing cloud security standards to the financial market. The latter suggest a clear awareness gap since governance and assurance standards specifically developed for and aimed at the cloud already exist, and some of them are considered mature enough to be adopted. ISO 27001[45] and PCI-DSS[46] are the most commonly used standards, but various FIs express that cloud-specific certification frameworks would be a more helpful approach to compliance.

Additionally, ENISA has developed two specific tools for supporting security awareness in the cloud:

- Cloud Certification Schemes List (CCSL)[47] is a list of existing certification schemes relevant to cloud computing customers. CCSL provides potential customers with an overview of objective characteristics per scheme, to help them understand how the scheme works and if it is appropriate for their setting. CCSL is being improved continuously and updated by ENISA and stakeholders from industry and public sector.

- Cloud Certification Schemes Metaframework (CCSM)[48], is a framework that collects public sector security requirements and groups them into 27 security objectives. These security objectives are then mapped against the cloud certification schemes included in the CCSL. The goal of CCSM is to provide more transparency and help customers in the public sector with their procurement of cloud computing services.

Furthermore, experience of CSPs shows that for FIs sometimes the biggest obstacle in overcoming the risk of cloud computing comes from the misconceptions about the technology. It behoves CSPs to be more transparent about their cloud offerings.

45 http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
46 https://www.pcisecuritystandards.org/security_standards/index.php
47 https://resilience.enisa.europa.eu/cloud-computing-certification
48 https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework

4.2 Mitigation Measures

To mitigate the risks introduced by adoption of cloud computing, FI's willingness to engage has much to do with whether the cloud services offer specific functions and features. Some of these functions and features are needed for improving trust, and others are needed for security and compliance purposes.

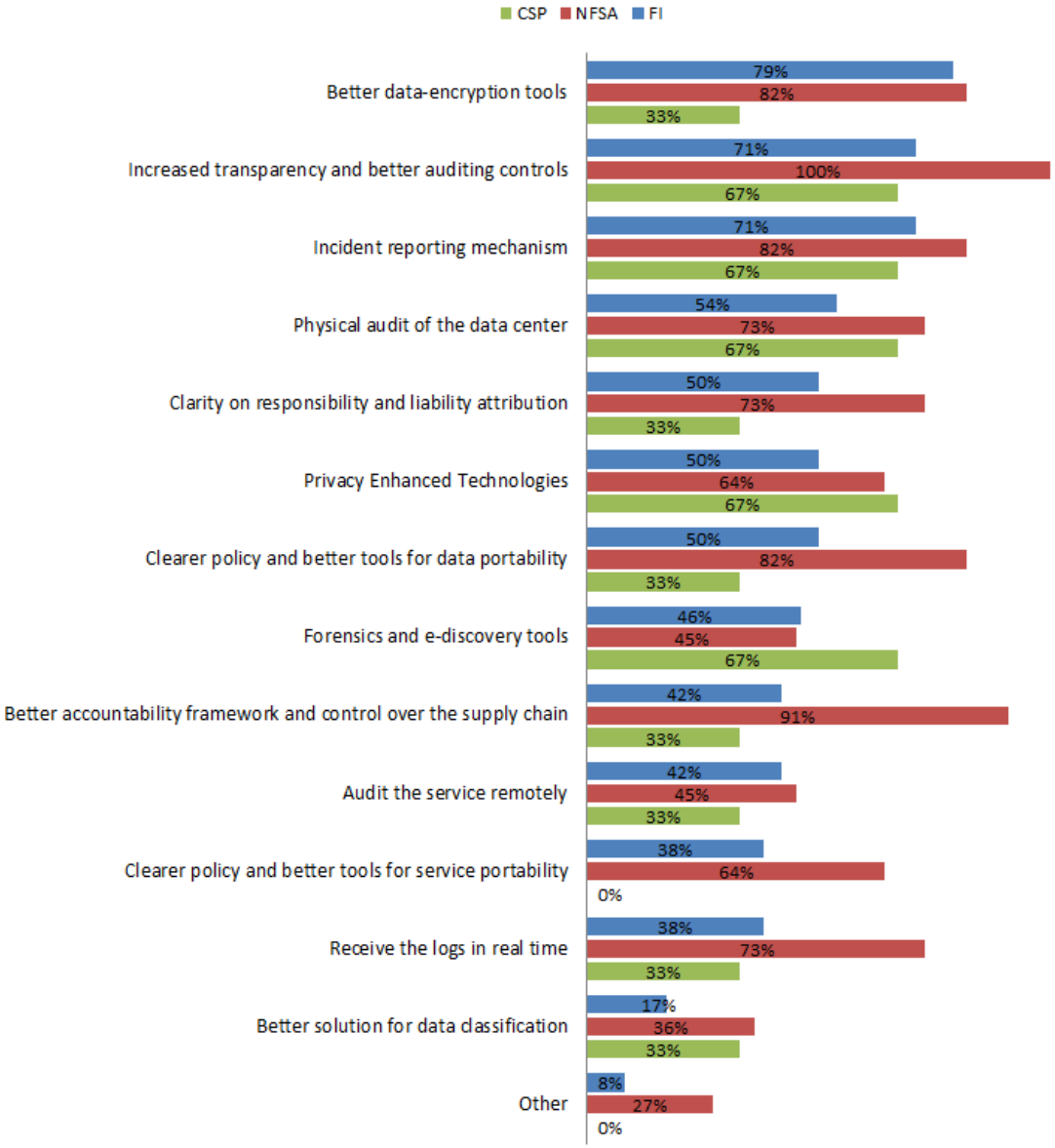

Figure 11 - Top features desired from cloud providers

The top desired features are depicted in Figure 11. NFSAs would generally desire more security features than the FIs, however the only area where NFSAs are less interested was forensics and e-discovery. FIs consider those features as important. CSPs noted that the majority of desired features shown in Figure 9 are being driven by privacy requirements.

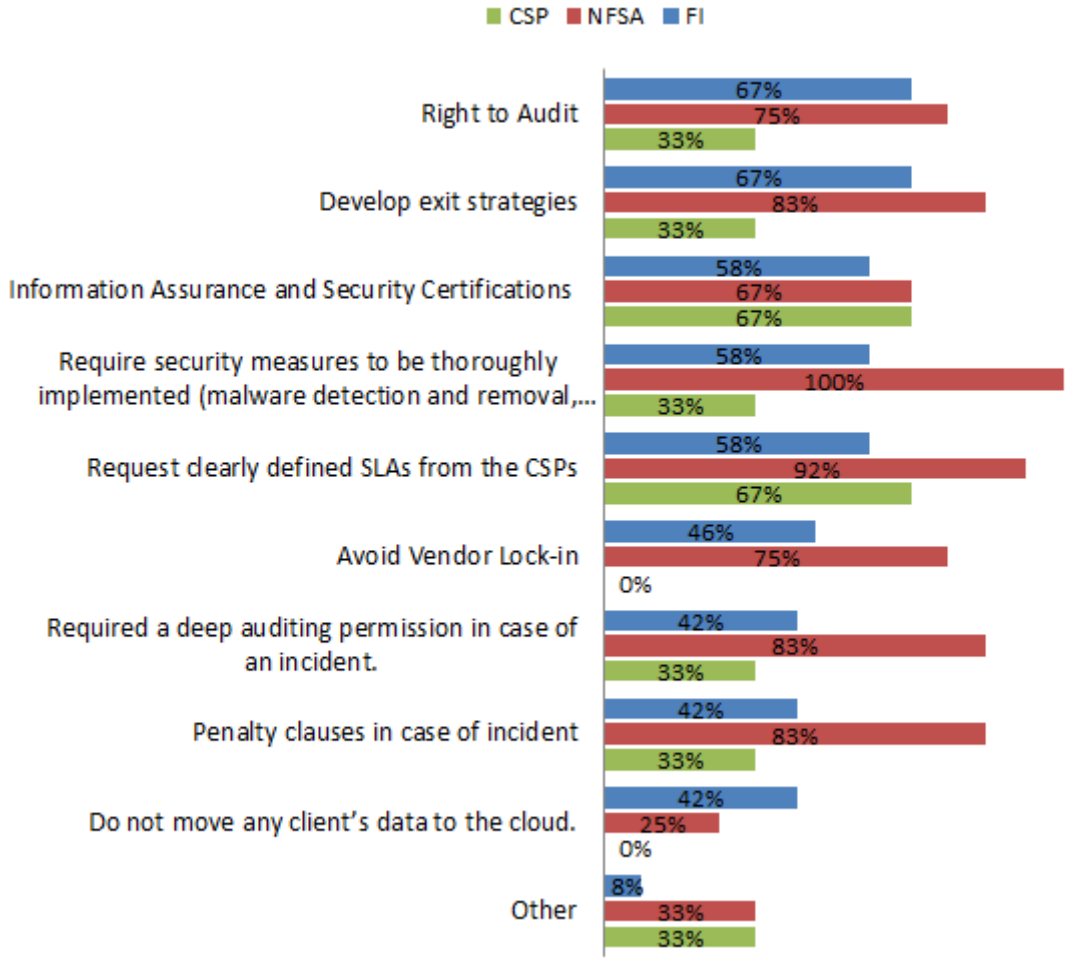

Figure 12 - Mitigation measures adopted

When asked about the mitigation measures implemented during migration to cloud services, the majority of respondents requested from their CSPs specific contract clauses such as right to audit, develop exit strategies, require information assurance and security certifications, thoroughly implemented security measures and clearly defined SLAs. It is clearly visible that NFSAs want a much stricter approach than the FIs are taking, although this should be noted as normal as this is due to their nature being not for profit, but prudence based. However, they are much less reluctant about moving client (vs. the FI's) data to the cloud, assuming that a risk assessment has been performed and the risks adequately mitigated. The percentage of FIs who have not moved client data to the cloud is consistent with the number of FIs who have not developed a detailed corporate risk assessment for cloud based services (Figure 7).

We conclude from this data that some FIs are making *a priori* decisions about not using the cloud for sensitive data rather, than basing their decision on a mature analysis and assessment of the risks.

5. Recommendations

In this section we provide a list of recommendations addressed mainly to FIs and regulators. The recommendations are grouped into four key areas: collaboration, risks based approach, transparency and assurance and information campaigns.

5.1 Cooperation between FIs, NFSA and CSPs

This study highlights the fact that in countries where there is effective communication and collaboration between FIs, NFSAs and CSPs the cloud market is able to evolve more quickly. Therefore we recommend that FIs to engage with CSPs and NFSAs, with the following objectives:

1. NFSAs to define national good practices and (de-facto) standards in the areas of cloud governance and risk management for the adoption of Cloud computing in the finance sector.

2. NFSAs to define good practices and de-facto standards for incident information sharing. On-going efforts, such as those conducted at the Financial Services Information Sharing and Analysis Center (FS-ISAC), have limitations both in terms of geographic spread and in level of details of the information being shared. Therefore NFSAs with the help of FIs and CSPs should focus on mechanisms to increase the level of trust between the members of the information sharing platform, and consequently increase the amount and level of detail of the incident information.

Referring to the previous point, we recommend that NFSAs work together at the global and European levels to define a set of common good practices for cloud security and privacy. Priority should be given to:

3. NFSAs with the help of EU Institutions (EBA, EC) to create harmony between legal and regulatory requirements. We recommend a consolidated approach to regulation of cloud computing in Europe. While supervisory authorities in Europe seem to have similar attitude with regards to cloud computing, their approach to the regulation varies significantly. Harmonising current national legislations, and defining baseline requirements and guidance on cloud computing throughout the European finance sector, would decrease the effort required for all parties involved. It would also provide much needed clear/formal regulatory positions on cloud computing to FIs, which would enable successful cloud adoption projects across multiple regulatory jurisdictions in Europe. Furthermore, with clear and consolidated guidance from supervisory authorities, FIs will be able to develop detailed corporate risk assessments and strategies for cloud computing, while clearly understanding the prudential statutory and subsidiary legislation relevant to the subject of cloud computing. Baseline regulatory requirements should addressing confidentiality, integrity, availability and location of data. Contractual right to audit clauses should be considered as a baseline assurance mechanism for FIs. Supervisory authorities should agree on a consensus approach to oversee CSPs, ideally through existing assurance mechanisms available in the industry, coupled with additional guidance specific for financial industry.

4. Minimum security and privacy requirements for the adoption of cloud based services: We recommend that regulators work on the definition of the security and privacy requirements/principles that should be adopted by FIs when adopting cloud services. Those requirements should reflect the different level of service criticality and impact (e.g., a service moderate impact would require the implementation of baseline requirements). The definition of criticality / impact levels for services and corresponding security and privacy requirements would offer several benefits such as:
    a. Support smaller FIs and CSPs in their cloud risk assessment and management approach

b. Help CSPs develop a standard offering depending on the level of criticality of services
c. Provide FIs and CSPs with a uniform set of baseline security requirements to support the security interoperability between services

Organisations such as ENISA Information Assurance Framework[49)], and NIST SP 800-53 Rev. 4[50] have already developed security controls frameworks that are sufficiently mature and could be used to derive minimum security and privacy requirements for the finance sector. An increased collaboration between NFSAs is desirable also in relation to cloud systemic risks we referred to earlier.

5. Policy makers (EC, EBA, ENISA) to identify existing and/or create new European / global mechanisms for security and privacy compliance, including possible further enhancements of existing certifications and certification practices.

5.2 Risk-based approach (risk assessment/cloud strategy)

6. We recommend that FIs develop a cloud computing strategy in order to define their approach to cloud computing. Organisations should adopt a risk-based approach when moving to the cloud, and their strategy should be aligned with their corporate risk assessment. By understanding and evaluating their assets they will be able to assess confidentiality, integrity and availability requirements for deployment of cloud services within their organisation. Based on the security and risk requirements, organisations should have a good idea of their comfort level for transitioning to the cloud, and which combinations of deployment, service models and locations fit their risk tolerance. We recommend that FIs perform a corporate risk assessment on cloud computing by using their corporate risk assessment framework, and by leveraging existing cloud specific tools and methodologies.

5.3 Transparency & Assurance

7. In the section on Information Campaigns, we highlight the need to better inform both regulators and FIs about the security risks and opportunities connected to the use of cloud computing. We believe that both FIs and NFSAs are overly cautious in their approach to cloud computing due to misconceptions about the technology. In order to address this issue, an increased level of transparency and trust is needed. Thus, we recommend that CSPs continue their efforts to provide sufficient transparency and help their customers and supervisory authorities understand the level of assurance that their cloud offerings provide. Such an effort should be based on:

a. Mechanisms that align the classification of assets (services and information) of the customer with the classification adopted by CSPs.
b. Information sharing about CSPs risk management process.
c. Statements and Service Level Agreements (SLAs) on security and privacy controls applied to the service provided. These SLAs should be simple, unambiguous, measurable and comparable.
d. Right to audit, or alternatively show adherence to suitable security and privacy standards through certification (or 3rd party assessment). This should be required especially in the cases of critical services.
e. Create specific information documents addressed to supervisory authorities and financial service risk/security/compliance/audit officers.

49 https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport. Last accessed 15th September 2015
50 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Last accessed 15th September 2015.

It is important to note that there is no single solution, and the recommendations made above can be considered as the main building blocks to achieving sufficient level of transparency and trust in the finance sector.

5.4 Information campaigns

8. We recommend that the European Commission, other relevant European Agencies (e.g., EBA, ENISA) as well as industry bodies work together to create information campaigns for the financial industry with the following objectives:

    a. Increasing the understanding of the NFSAs, other financial regulators and FIs on cloud based services and their connected security risks as well as security benefits
    b. Clarifying the differences between cloud based services and outsourcing
    c. Clarifying the trade-offs between Public cloud, Private cloud, outsourcing and in-house IT
    d. Explaining the tools, techniques, certifications, good practices and standards that, if adopted, could facilitate safe adoption of cloud based services
    e. Clarifying the role that security and privacy certifications could have on increasing the level of trust in cloud services. As a starting point we recommend using specific tools, such as CCSL and CCSM developed by ENISA, which will promote and understanding of the characteristics of certification schemes, and how they accomplish security objectives.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-02-15-840-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-138-0
DOI: 10.2824/199301