OUTSOURCING TO THE CLOUD: EIOPA'S CONTRIBUTION TO THE EU COMMISSION FINTECH ACTION PLAN

https://eiopa.europa.eu/

eiopa
European Insurance and
Occupational Pensions Authority

PDF	ISBN 978-92-9473-145-6	doi:10.2854/774288	EI-03-19-155-EN-N
Print	ISBN 978-92-9473-144-9	doi:10.2854/424430	EI-03-19-155-EN-C

Luxembourg: Publications Office of the European Union, 2019

OUTSOURCING TO THE CLOUD: EIOPA'S CONTRIBUTION TO THE EU COMMISSION FINTECH ACTION PLAN

Data updated as at 31 December 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The European Commission FinTech Action Plan requires the European Supervisory Authorities (ESAs) to explore the need for guidelines on outsourcing to cloud service providers by Q1 2019.

In the European financial regulatory landscape, the purchase of cloud computing services falls within the broader scope of outsourcing.

The credit institutions, investment firms, payment institutions and the e-money institutions have multiple level 1 and level 2 regulations that discipline their use of outsourcing (e.g. MIFID II, PSD2, BRRD). There are also level 3 measures: CEBS[1] Guidelines on Outsourcing, representing the current guiding framework for outsourcing activities within the European banking sector.

Additional "Recommendations on cloud outsourcing" were issued on December 20, 2017 by the European Banking Authority (EBA) and entered into force on July 1, 2018. They will be repealed by the new guidelines on Outsourcing Arrangements[2] (level 3) which have absorbed the text of the Recommendations.

For the (re)insurance sector, the current Regulatory framework of Solvency II (level 1 and level 2) discipline outsourcing under Articles 38 and 49 of the Directive and Article 274 of the Delegated Regulations. The EIOPA guidelines 60-64 on System of Governance provide level 3 principle based guidance.

On the basis of a survey conducted by the National Supervisory Authorities (NSAs),[3] cloud computing is not extensively used by (re)insurance undertakings: it is most extensively used by newcomers, within a few market niches and by larger undertakings mostly for non-critical functions. Moreover, as part of their wider digital transformation strategies many European large (re)insurers are expanding their use of the cloud.

As to applicable regulation, cloud computing is considered as outsourcing and the current level of national guidance on cloud outsourcing for the (re)insurance sector is not homogenous[4]. Nonetheless, most NSAs[5] (banking and (re)insurance supervisors at the same time) declare that they are considering the EBA Recommendations as a reference for the management of cloud outsourcing.

---

1 Committee of Banking Supervisors – predecessor of EBA.

2 The EBA guidelines on Outsourcing Arrangements were issued in draft version on June 22, 2018 and will repeal the CEBS Guidelines on outsourcing (consultation phase ended on 24 September 2018)

3 The list of the NSAs is provided at Annex 2 and Annex 3

4 In CZ, DE, FI, FR, PL, SE, UK-FCA, national guidance on cloud outsourcing applicable to the financial sector including (re)insurance have been published by the NSA.

In ES, IT, LV, RO, FR, NL, there are broader national standards to support the management of specific critical areas of cloud outsourcing.

In GR, PT and IE there is not a specific plan.

5 DE, FI, GR, IE, LT, NL, SE, UK

According to the results of the survey, the usage of cloud computing services by (re) insurance undertakings is aligned to the banking sector. The risks arising from the usage of cloud computing by (re)insurance undertakings appear to be, generally, aligned to the risks borne by banking players[6] with few minor (re)insurance specificities.

In light of the above considerations, to support market participants (i.e. regulated undertakings and service providers)[7] and to avoid potential regulatory arbitrage,[8] EIOPA has decided to prepare guidance on cloud outsourcing aligned with the EBA Recommendations with minor amendments to reflect the (re)insurance specificities highlighted by the analysis carried out.

Under the steering of its InsurTech TaskForce, EIOPA will develop its own Guidelines on Cloud Outsourcing.

The intention is that the Guidelines on Cloud Outsourcing (the "guidelines") will be drafted during the first half of 2019, issued then for consultation and finalised by the end of the year.

During the process of drafting the Guidelines, EIOPA will organize a public roundtable on the use of cloud computing by (re)insurance undertakings. During the roundtable, representative from the (re)insurance industry, cloud service providers and the supervisory community will discuss views and approaches to cloud outsourcing in a Solvency II and post-EBA Recommendations environment.

Furthermore, in order to guarantee a cross-industry harmonization within the European financial sector, EIOPA has agreed with the other two ESAs:

- to continue keeping the fruitful alignment kept so far; and
- to start – in the second part of 2019 – a joint market monitoring activity aimed at developing policy views on how cloud outsourcing in the finance sector should be treated in the future. This should take into account the increasing use of the cloud and the potential for large cloud service providers to be a single point of failure.

6 For the purpose of this document, banking players are the undertakings defined under the article 4(1) of the Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR)

7 5 National Supervisory Authorities to the question "Do you think that this topic needs to be clarified to support the market participants?" replied "YES"

8 5 National Supervisory Authorities to the question "Do you think that more clarity on this could avoid a potential regulatory arbitrage on cloud outsourcing?" replied "YES"

INTRODUCTION AND OBJECTIVES

The FinTech[9] Action Plan published by the European Commission (from now on "EC" or "Commission") on March 3, 2018 combines both supportive measures to help introduce FinTech solutions and proactive measures to foster and stimulate new solutions and address in a determined way the emerging risks and challenges.

Within this publication, the Commission has set out its plans for further work on enabling, accommodating and, where possible, encouraging innovation in the financial sector, while ensuring at all times the preservation of financial stability and high levels of investor and consumer protection.

The goals of the Action Plan are threefold:

1. to harness rapid advances in technology for the benefit of the EU economy, citizens and industry,
2. to foster a more competitive and innovative European financial sector, and
3. to ensure the integrity of the EU financial system.

Cloud computing is one of the technological innovations in the financial sector that were put under the Commission spotlight within the Action Plan.

While the Commission recognises the potential of cloud computing for the financial services sector, it underlines some concerns related to uncertainties of its interpretation by financial supervisory authorities within the scope of outsourcing requirements imposed on the undertakings.[10]

Within this scope, **the Commission has invited the ESAs to explore the need for guidelines on outsourcing to cloud service providers by Q1 2019**.

Structure of the document

This document is composed by three sections and an executive summary.. At the end of each section, where relevant, the key takeaways are summarized within blue text boxes.

The three sections are structured as follow:

1. Overview of cloud computing.
2. Overview of market practices on cloud computing, drilling down on the following areas:
   - a status update of the other ESAs' work on cloud computing;
   - an analysis of the current EU (re)insurance regulatory framework;
   - the results of the light assessment performed by the ITF members;
   - examples on the use of cloud computing within the financial industry.
3. Summary of key takeaways and EIOPA's answer to the European Commission.

9 FinTech is a term used to describe technology-enabled innovation in financial services that could result in new business models, applications, processes or products and could have an associated material effect on financial markets and institutions and how financial services are provided

10 Regulated firms that outsource activities to a cloud service provider must comply with all legal requirements (e.g. in terms of proper risks management, data protection and appropriate oversight by supervisors). Stakeholders responding to the Commission consultation raised concerns that uncertainties over financial supervisory authorities' expectations were limiting the use of cloud computing services. Such uncertainties are due in particular to the absence of harmonisation of national rules and different interpretations of outsourcing rules.

1. OVERVIEW OF CLOUD COMPUTING

The purpose of this section is to build up a common understanding of what is generally meant by cloud computing. It contains also a high level costs/benefits analysis related to its adoption. The definitions and the approaches here reported do not, necessarily, represent the ones for the (re)insurance sector.

Cloud computing technology has become increasingly widespread since the late 2000's and adoption of cloud computing services has been growing steadily, in all sectors of the economy and by all economic operators.

In order to build up a common playground on this subject, the paragraphs below provide a set of definitions and highlight some of its features.

Moreover, at the end of the paragraph is provided a summary of the main different incentives for a financial undertaking (including the insurance and reinsurance undertakings) to invest in its own data centre or rely upon cloud computing.

1.1 DEFINITIONS

Cloud computing allows users to access on-demand, shared configurable computing resources (such as networks, servers, storage, applications and services) hosted by third parties on the internet, instead of building their own IT infrastructure

According to the US National Institute of Standards and Technology (NIST), cloud computing is:

> "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

The ISO standard of 2014 defines cloud computing as a:

> "paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand". It is composed of "cloud computing roles and activities, cloud capabilities types and cloud service categories, cloud deployment models and cloud computing cross cutting aspects".

The European Banking Authority (EBA) Recommendations of 2017 defines the cloud services as:

"Services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [11]

Essential Characteristics

According to the NIST, the cloud computing model is composed of five essential characteristics, three service models, and four deployment models.

Cloud computing essential characteristics are the following:

a) **On-demand self-service**

A cloud customer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

b) **Broad network access**

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

11 In order to ensure consistency, for the further developments on cloud outsourcing, EIOPA will use the definition provided by the EBA Recommendations.

c) **Resource pooling**

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to customer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

d) **Rapid elasticity**

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the customer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

e) **Measured service**

Cloud systems automatically control and optimize resource use by leveraging a metering capability some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and customer of the utilized service.

Service models

Cloud computing has been developing along the following three main concepts:

a) **Infrastructure as a Service (IaaS)**

The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software. It can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).

b) **Platform as a Service (PaaS)**

The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

c) **Software as a Service (SaaS)**

The capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.

Deployment models

These cloud services are, generally, deployed through the following models:

a) **Private cloud services**

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

The EBA Recommendations defines the private cloud services as "cloud infrastructure available for the exclusive use by a single institution."

b) **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, and it may exist on or off premises.

The EBA Recommendations defines the community cloud services as "cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group."

c) **Public cloud services**

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Public cloud services may be free or offered in a pay-per-usage or other service fee models.

The EBA Recommendations defines the public cloud services as "cloud infrastructure available for open use by the general public".

d) **Hybrid cloud services**

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between cloud).

The EBA Recommendations defines the hybrid cloud services as "cloud infrastructure that is composed of two or more distinct cloud infrastructures."

1.2 CLOUD COMPUTING: A SHARED RESPONSIBILITY MODEL

Actors in cloud computing

According to the NIST cloud reference architecture, the following five are the major actors to be taken into account when cloud computing is under examination.

a) **Cloud Customer (or "Cloud User")**

The cloud customer is the principal stakeholder for the cloud computing service. A cloud customer represents a person or organization that maintains a business relationship with and uses the service from a cloud provider.

A cloud customer browses the service catalog of a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service.

b) **Cloud Provider**

The cloud provider is a person, organization or entity responsible for making a service available to interested parties.

A cloud provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the cloud customers through network access.

c) **Cloud Auditor**

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon.

Audits are performed to verify conformance to standards through review of objective evidence.

A cloud auditor can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

d) **Cloud Broker**

An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud customers. A cloud customer may request cloud services from a cloud broker, instead of contacting a cloud provider directly.

e) **Cloud Carrier**

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud customers and cloud providers. Cloud carriers provide access to customers through network, telecommunication and other access devices. For example, cloud customers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices, etc.

Usually, a cloud provider set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud customers. Moreover, the cloud provider may require the cloud carrier to provide dedicated and secure connections between cloud customers and cloud providers.

Shared responsibility framework[12]

The cloud provider and cloud customer share the control of resources in a cloud system. The cloud's different service models affect their control over the computational resources and, thus, what can be done in a cloud system.

Compared to traditional IT systems, where one organization has control over the whole stack of computing resources and the entire life-cycle of the systems, cloud providers and cloud customers collaboratively design, build, deploy, and operate cloud based systems.

The split of control means that both parties share the responsibilities in providing adequate protections to the cloud-based systems. The picture below[13] shows, as "conceptual model", the different level of sharing responsibilities between the cloud provider and the cloud customer.

These responsibilities contribute to achieve a compliant and secure computing environment.

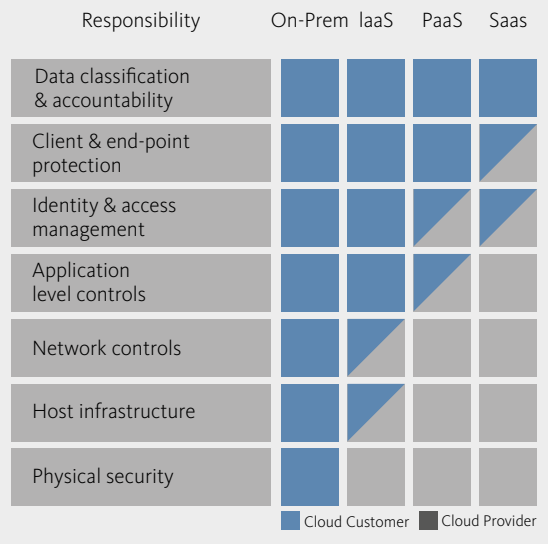
It has to be noted that, regardless the service provided by the cloud provider:

- Ensuring that the data and its classification are done correctly and that the solution is compliant with regulatory obligations[14] is the responsibility of the customer[15] (e.g. in case of data theft the cloud customer is responsible towards the damaged parties or the customer is responsible to ensure – e.g. with specific contractual obligations – that the provider observe certain compliance requirements such as give the competent authorities access and audit rights);
- Physical security is the one responsibility that is wholly owned by cloud service providers when using cloud computing.

The remaining responsibilities and controls are shared between customers and cloud providers according to the outsourcing model. However, the responsability (in a supervisory sense) remains with the customers. Some responsibilities require the cloud provider and customer to manage and administer the responsibility together including auditing of their domains.

For example, identity & access management when using a cloud provider's active directory services could require that the configuration of services such as multi-factor authentication is up to the customer, but ensuring effective functionality is the responsibility of the cloud provider.

Picture 1 Shared responsibilities for different cloud service models



12 The shared responsibility model here represented is a conceptual model and it is depicted for illustration only. Moreover, it has to be noted that the concept of "responsibility" here depicted it is not affect the responsibilities of a (re)insurance undertaking toward its stakeholders (i.e. customers, regulators and the market in general)

13 "Shared Responsibilities for Cloud Computing", Microsoft, April 2017.

14 Such as: (i) multiple EU non-financial specific Regulations (e.g. the EU 2016/679 "General Data Protection Regulation" and the Proposal for a regulation on a framework for the free flow of non-personal data in the European Union, EU/US Privacy Shield) (ii) financial specific regulations (e.g. Directive 2009/138/EC "Solvency II"; Directive 2014/65/EU "Mifid 2"; etc.).

15 Notwithstanding the sentence in the body text, in the case of the General Data Protection Regulation (GDPR), the processor (in this case, the cloud provider) must also be compliant when personal data is processed.

1.3 INCENTIVE TOWARDS INVESTING ON MODERN CORPORATE DATA CENTERS VS. OUTSOURCING TO THE CLOUD

Modern corporate data centres

Most financial firms, including financial market infrastructures and (re)insurance undertakings, have invested in and continue to operate corporate data centres that were designed as fit-for-purpose for the specific needs of a particular business.

Both existing corporations and newly formed start-ups must weigh the costs and benefits of leveraging a corporate data centre or using the cloud.

On top of the advantage of limiting outsourcing risks related to a third party service providers, here below are reported some other advantages and benefits to private, corporate infrastructure that may compel some companies to maintain or expand their own data centres (the following are mostly valid also for outsourced data centres). These include:

- Proprietary configurations or specialized systems that might be not available at public cloud vendors (nonetheless, in case of certain cloud solutions, a cloud customer does not have necessarily to use the software or systems of a cloud provider he can still use its own IT-infrastructure and just link this to a cloud (via Application Program Interface, or API) for processing and data storing);
- Dedicated resources;
- Situations that require as business as usual highest performance requirements, extremely low latency or massive data processing (on the other hand, usage of cloud computing could be beneficial in case of peaks, which do not occur regularly, can be absorbed by a cloud service while the customer has not to undertake high investments in its own data centres).

It is also true that some existing applications, where on-premises systems may have already been optimized and given increased efficiency, may not gain any benefits from moving to the cloud, apart from of the possible reduction of costs and the use of the technical expertise of the cloud computing providers.

Much of today's legacy infrastructure was built with a purposeful and intentional design to support a set of applications at a given point in time. As a result, firms face increasing financial, security and other issues because the simplicity of the initial designs have become enormously complex due to continuous waves of mergers, integrations, enhanced security requirements and rushed additions or modifications. Many modern corporate data centers present the following common set of challenges that could lead to the use of a cloud solution:

a) **Complexity challenge**

This is the result of the ever-expanding portfolio of hardware components, network segments and software products created, purchased or acquired over the course of years. Retiring or removing technology is difficult and often results in unexpected disruptions, which means that many firms have an inventory of applications and hardware that are unused but still online. Business continuity requirements, which are typically achieved through multiple data centers, replication schemes and tightly orchestrated recovery scripts, add to the complexity

b) **Security challenge**

Legacy infrastructures were often not architected with centralized controls or logging and management consoles. In addition, they typically provide limited, if any, information about their running status. The challenges are compounded with older networks that were not designed and built with network and end point security, which put them at increasing risk from external access and unknown actors. Patching mixed environments to prevent the latest security exposures is time consuming and difficult and could be very expensive. Furthermore, for some older systems, security patches might not be provided by the tech-support anymore, if these were bought from a third-party

c) **Cost challenge**

Maintaining a corporate data center has become an expensive proposition for many financial undertakings as they are forced to invest limited resources into: hardware refresh and their related depreciation, purchasing and maintaining unused excess capacity to support the highest-ever projected volume requirements, purchasing and maintaining unused excess capacity to support local component failure and out-of-region disaster recovery and all of the human and organizational resources to manage and maintain these assets.

On the other hand, FinTech start-ups that have to build up their entire IT infrastructure landscape have more flexibility to decide whether (or not) invest in traditional IT systems and data centers to support their business models in house or through dedicated data centers outsourcing.

In their case, the incentives to invest are mainly aligned with the ones reported above while the issues are mostly related to the cost challenges (in their case, the complexity challenge can be considered as a component of the cost challenge).

Outsourcing to the cloud

Outsourcing to cloud, particularly when it is deployed toward a public cloud infrastructure, provides services and capabilities that mitigate many of the challenges presented above.

Scale

- The cloud provides the impression of nearly unlimited capacity as a result of vast resource shared across millions of users.
- Cloud customers can use the "auto-scaling" features to automatically scale up when additional capacity or performance is needed and scale down when demand subsides.
- Storage is provided at the time it is needed, with the required performance and cost. Overprovisioning is eliminated, potentially saving users a significant amount of money.

Resiliency

The cloud provides expanded models for building applications that must be constantly online, and designing systems resilient to disruption when components fail or changes are introduced. Some examples include:

- auto-scaling;
- load balancing applications across data centers and geographic regions;
- distributing copies of applications to multiple domestic and global locations and turning them on or off as needed;
- changing and pre-validating in isolation, testing and scheduling the release.

The cloud providers's data centers are generally structured following an high level of standardization, so every location can be identically configured and automatically verify the same code and data. Thanks to this, operating from a "backup copy" of an application can be turned into an every day standard, instead of the complex, orchestrated event it is today in many "in house" solutions.

Privacy

Under the assumption that the data classification and accountability falls under the customers responsibility, the privacy design features of the public cloud enable financial undertakings to protect client data and address local jurisdictional rules regarding privacy.

For example, the foundation of the cloud is the internal walls that allow pooled (multi-tenancy) and shared resources (virtualization) to keep individual environments separate, independent and isolated from and unaware of each other, even if the same physical resources are shared.

In addition, unlimited 'private' segments can be created for network, compute and/or data resources while giving users access to a wide range of encryption technologies and tools that can be tailored to their specific requirements. Cloud vendors also provide data centers in many regional and global geographic areas to address regulatory requirements. Encryption keys can be managed by the financial undertakings, further securing access to client data.

Security

Since they have significant economic interests and incentives to prodect customers, the cloud service providers, in most cases, have built their infrastructure and service delivery models to support the most stringent security requirements at every level. For example: their security models can be established and enforced within applications using best practices, standards, data encryption, and API logging – all required and validated both by cloud customer and provider.

The use of public cloud vendors allows an enterprise to distribute encrypted applications and data across millions of servers in dozens of data centers, making it almost impossible to identify the physical resources being used by a specific firm.

Nowithstanding the above, it has to be noted that the use of cloud computing does not eliminate the security risks for the cloud customer.

Nonetheless, since cloud computing is a shared technology model – where different organizations are frequently responsible for implementing and managing different parts of the stack - from an operational perspective the security responsibilities are also distributed across the stack, and thus across the organizations involved.

Moreover, associated to the cloud there are many new and also older security vulnerabilities and threats, from governance related issues[16] to those related to the IT delivery and user access management.[17]

Cost & Time to Market

For most applications and configurations, the cloud will cost less[18]. The scale, resource sharing, automation and metering of resources consumed contribute to lowering the costs of technology infrastructure for typical system requirements. This allows for instant experimentation, immediate results, creating a dynamic culture where the user can test virtually any scenario, new software tool or alternative configuration without a lengthy purchase and provisioning cycle. These features support faster time to market, more reliable products and lower requirements for support and maintenance.

Moreover, the use of cloud computing extensively could enable the undertakings to be immediately able to scale their business at "regional" or "global" level faster and at lower costs than their competitors that rely upon a more traditional IT service model.

Summary

In summary, there are many benefits of building applications in the cloud, including faster time to market, lower development costs, expanded testing, enhanced controls, automatic scaling and failover and quicker provisioning.

However, just moving applications that were originally developed within the corporate data center to the cloud, a model known as "lift and shift," could not immediately deliver these benefits. In some cases, migrating to the cloud could introduce additional complexity.[19]

16 One of the most important security consideration is knowing exactly who is responsible for what in any given cloud project. It's less important if any particular cloud provider offers a specific security control, as long as you know precisely what they do offer and how it works. For this reason, according to the Cloud Security Alliance Among the most significant security risks associated with cloud computing there is the tendency to bypass information technology (IT) departments and information officers.

17 For example, the ability to deploy easily and simultaneously applications and tools provided by the cloud computing, could also be a vehicle for virus to get into the system and propagate very easily. For a more detailed list of cloud IT security threats, please refer to the CSA "Security Guidance for critical areas of focus in cloud computing" and the CSA "White paper – The treacherous 12, top threats to cloud computing + industry insights"

18 According to the Final Report of the study "SMART 2013/0043 - Uptake of cloud in Europe", the adoption of cloud computing services allow firms to reduce IT costs ranging from a 20% to 50% reduction and to shift IT costs from capital expenditure (CAPEX) to operating expenses (OPEX).

19 For example, there are risks associated with potential mutation of internal infrastructure for the insurers when they port to a cloud-based system.

2. OVERVIEW OF MARKET PRACTICES

2.1. SUMMARY OF ESAS' WORK ON CLOUD COMPUTING

All the European Supervisory Authorities (ESAs) have launched specific initiatives to answer the Commission request as presented at paragraph 1.

2.1.1 EUROPEAN BANKING AUTHORITY (EBA)

For the banking sector, on December 20, 2017 the European Banking Authority (EBA) published the "Recommendations on cloud outsourcing" which entered into force on July 1, 2018.

The baseline guidance for the Recommendations was the CEBS[20] Guidelines on Outsourcing which were issued in 2006 and represents the current guiding framework that regulates outsourcing activities for the banking sector.[21]

Both the EBA Recommendations and the CEBS Guidelines on Outsourcing will be repealed by the new EBA guidelines on Outsourcing Arrangements (consultation paper was published by the EBA on June 22, 2018).

The Recommendations apply to credit institutions and investment firms as defined under the article 4(1) of the Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR).

The aims of the EBA Recommendations are to:

- provide the necessary clarity for institutions should they wish to adopt and reap the benefits of cloud computing while ensuring that risks are appropriately identified and managed;
- foster supervisory convergence regarding the expectations and processes applicable in relation to the cloud.

2.1.2 EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA)

The European Securities and Markets Authority (ESMA) has not issued specific guidelines on cloud computing. For the sectors supervised by ESMA,[22] the practice of using cloud computing services falls within the outsourcing scope that is regulated by the sectoral level 1 and level 2 regulations. As part of its work relating to the FinTech Action Plan, in 2018 ESMA analysed the use of cloud computing by its directly-supervised entities (CRAs and TRs). ESMA is observing an increase in the use of cloud services by supervised entities, especially larger such entities.

ESMA is currently considering whether to issue guidelines on the use of cloud computing for entities within its remit and will communicate with the Commission on this matter in due course.

20 Committee of Banking Supervisors

21 The EBA, as mentioned previously, has recently issued a consultation version of the new Guidelines on Outsourcing Arrangements that will repeal the CEBS Guidelines and the Recommendations on Outsourcing to the Cloud (references are reported at Annex 1)

22 ESMA performs direct supervision on Credit Rating Agencies (CRAs) and Trade Repositories (TRs). For the other financial market participants (i.e. CCPs, CSDs, Trading Venues, Investment Firms, data service providers, asset managers), the ESMA role is aligned to the one of the other ESAs.

2.2. SELECTION OF OTHER INTERNATIONAL SUPERVISORS / AUTHORITIES WORK ON CLOUD COMPUTING

The Financial Stability Institute (FSI) hosted by the Bank for International Settlements (BIS) has undertaken a stocktake of (re)insurance regulatory and supervisory approaches to outsourcing to technology service providers, including specific recommendations or guidelines for cloud computing services. EIOPA has also been involved in this exercise.

Output of the exercise was a research paper on cloud computing to provide an overview on selected regulatory frameworks (including some EU jurisdictions but not limited to them) and on emerging regulatory practices. This research paper was published on December 5, 2018.

The Organization for Economic Cooperation and Development (OECD) published a report on cloud computing on August 19, 2014.[23] This report provides an overview of the main challenges for policy makers related to cloud computing such as: data privacy, security and risk management, lack of appropriate standards (for instance to avoid vendors lock-in), contractual issues. Other challenges related to government policy are lack of adequate broadband infrastructure, trade and competition implications, tax implications, etc.

Moreover, a number of supervisory authorities outside the EEA have issued guidance on cloud.

- The Australian Prudential Regulation Authority (APRA) has issued on July 6, 2015 an information paper on Outsourcing involving shared computing services (including cloud);
- The Monetary Authority of Singapore (MSA) has issued on July 27, 2016 the "Guidelines on outsourcing" which also deal with cloud computing;
- The Office of the Superintendent of Financial Institutions (OFSI) of Canada in 2009 has revised guideline related to Outsourcing of Business Activities, Functions and Processes applicable to cloud computing.

23 OECD, Directorate for Science Technology and Industry – Committee on Digital Economy Policy, Cloud Computing: The Concept, Impacts, and the Role of Government Policy, August 19, 2014.

2.3. CURRENT EU REGULATORY FRAMEWORK

2.3.1 OUTSOURCING TO THE CLOUD WITHIN THE SOLVENCY II FRAMEWORK

Within the Solvency II framework the cloud outsourcing topic is managed by the provisions related to the outsourcing[24] contained within:

- Article 38 of Directive 2009/138/EC (to follow "Article 38")
- Article 49 of Directive 2009/138/EC (to follow "Article 49")
- Article 274 of Delegated Regulation 2015/35 (to follow "Article 274")

Those provisions are further detailed and clarified by the EIOPA guidelines on system of governance nr. 60-64 (to follow "guidelines" or "GL").

2.3.2 EBA RECOMMENDATIONS VS. SOLVENCY II

The Solvency II framework (Directive, Delegated Regulations and Guidelines) covers most of the contents of the EBA Recommendations already by the articles related to outsourcing. Nonetheless, the EBA recommendations appear to be more specific about:

- execution of the materiality assessment on the services outsourced;
- registration of outsourcing arrangements / providers[25] (i.e. there is a specific requirement to build a register of all the cloud service providers. The Recommendations contains also the list of information to be included within in the register);

24 According to Article 13 (28) of the Directive 2009/138/EC "outsourcing" means an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself.

25 According to the draft EBA guidelines on outsourcing arrangements, where the register of all existing outsourcing arrangements, is established and maintained centrally within a group, the competent authorities, all institutions and payment institutions should be able to obtain their respective individual register without undue delay and it should be ensured by the institution or payment institution that all outsourcing arrangements, including outsourcing arrangements with service providers inside the group, are included in their individual register.

- duty to inform supervisors, the register mentioned at the previous point, should be made available to the competent authorities. According to the draft EBA guidelines on outsourcing arrangements, this register is to be made available in a common data base format;
- the access and audit rights for the undertakings including provisions to use audit tools: (a) pooled audits; (b) third party certifications; (c) third party or internal reports made available by the cloud service provider;
- how to deal with specific risks of cloud outsourcing such as: (i) security of IT data and systems; (ii) location of data and data processing; (iii) chain outsourcing; and (iv) contingency plan and exit strategy.

TAKEAWAYS: Both banking and (re)insurance regulations discipline cloud computing by their current outsourcing provisions.

The Solvency II framework can be applied to most of EBA's Recommendations on outsourcing to cloud service providers already at level 1 and 2 within the provisions related to outsourcing. Annex 4 contains the gap analysis performed.

2.4. INSURANCE NATIONAL SUPERVISORY AUTHORITIES ON CLOUD OUTSOURCING

To build up a common understanding of the current status, EIOPA has gathered information on cloud computing with:

1. Questionnaire to the InsurTech Taskforce (ITF) members on specific cloud outsourcing aspects (definitions and national guidance);
2. Questions related to the use of cloud outsourcing in the industry survey on big data analysis in Motor and Health insurance;
3. Survey to assess whether risks arising from the use of cloud computing are different for banking and (re) insurance undertakings.

2.4.1 CLOUD COMPUTING DEFINITION AND NATIONAL GUIDANCE

The questionnaire shared among ITF members covers the following main aspects:

- Definition of cloud outsourcing

  To understand (i) whether (or not) cloud computing is considered outsourcing; and (ii) the current practices for its classification as "critical" or "important" by local undertakings[26]
- Presence of national guidance on outsourcing to the cloud
- Supervisory experience on issues associated to cloud computing

Annex 2 contains the list of the 17 NSAs from 16 jurisdictions that answered the questionnaire.

Definition of cloud outsourcing

For 11 of the NSAs cloud computing falls always within the broader category of outsourcing. Some NSAs have adopted a specific definition for cloud computing.

26 The question was developed, considering: (i) the Solvency II requirements on materiality assessment to be performed on the outsourced function or activity by the (re)insurance undertakings and (ii) under the assumption that the cloud computing falls within the broader outsourcing scope.

	Definition of cloud computing according to:				
	EBA	**ISO Std.**	**NIST Std.**	**Self-definition**	**No definition**
Cloud computing is ALWAYS outsourcing	GR, IE, UK PRA	ES,	CZ, PL, UK-FCA, NL	FI, FR[1], DE[2]	IT[3], LV
Cloud computing is outsourcing on A CASE BY CASE approach				RO	AT,SE
NA					PT

In case undertakings decide to outsource to a third party provider (or within the Group) an activity, they are required, by article 49 of the Solvency II-Directive, the article 274 of the Delegated Regulations and the EIOPA Guidelines on System of Governance article 60 to 64, to perform a materiality assessment of the service outsourced to understand if the service outsourced is "important" or "critical".

This shall be performed also for cloud computing.

The following practices (mutually not exclusive) have been reported:

- Cloud computing is always to be considered critical or important;
- Cloud computing is usually considered not critical or important;
- Cloud computing is classified on a case-by-case approach on the basis of the service/process/activity/data outsourced (this is the most adopted)

National Guidance on cloud outsourcing

The level of use of cloud outsourcing by (re)insurance companies differs among the EU jurisdictions:

- in some jurisdictions (e.g. AT, SE, NL) the use of cloud services is increasing;[30]
- in others (e.g. PT) it is not specifically addressed by the NSA or (e.g. in IT) it is common but not frequently used to support critical functions;
- in UK, cloud outsourcing has already had significant impacts in the banking industry and it is expected to have the same in the (re)insurance.

In light of the above, the current level of **national guidance on cloud outsourcing for (re)insurance sector is not homogenous**. Most of the NSAs declared that they are considering the EBA Recommendations as a reference for the management of cloud outsourcing.

- In some jurisdictions **national guidance on cloud outsourcing** applicable to the financial sector have already been published (CZ, FI, FR, PL, SE, UK-FCA) and in other the NSAs have committed to the issuance of them (DE[31])
- In other jurisdictions, there are **national standards** to support the management of specific critical areas of cloud outsourcing (e.g. security, data classification, IT Governance, outsourcing) (ES, IT,[32] DE, LV, RO, FR, NL)
- Some NSAs do not have specific plans (GR, PT, IE)

27 The following definition of cloud computing applicable France is a legal definition: "Method of processing a client's data, which are exploited via the Internet in the form of services provided by a service provider. Cloud computing is a special form of information technology (IT) outsourcing, in which end users are not informed of the location or internal structure of the cloud" → LINK.

28 The definition of cloud computing used by BaFin is not a legal definition and it is not adopted by the whole market. Bafin treats outsourcing to the cloud as outsourcing. Nevertheless, not every use of a cloud solution is outsourcing respectively subject to the specific outsourcing control (case by case approach is always necessary). In Germany, the following stages apply (see Margin no. 237 et seqq. of Circular 02/2017): (1) Segregation of outsourcing and other service relations (criteria are e.g. content, scope and duration of the relevant activity); (2) Outsourcing of a typical insurance function or activity; (3) Outsourcing of an important function or insurance activity. In general, each case has to be considered by the supervised entity

29 Within the Italian national regulation for the insurance sector there is no specific definition of cloud computing distinct from outsourcing which is defined and regulated according to the EU regulation. Ivass published in July 2018 an updated version of the governance requirements, including on outsourcing, cyber security and information technology.

30 In the NL, the usage of material cloud service is increasing. The amount of notifications to the DNB in 2017 have been doubled in comparison with 2016

31 BaFin: (i) Has published an article to provide some guidance and clarification to insurance companies (and companies of the banking sector) regarding cloud computing (Link); and (ii) Has published special guidance on the topic (Link).

32 Ivass reported that, in a recent seminar with firms on regulatory barriers to innovation, no specific mention was made on major impediments due to cloud regulation (or lack thereof).

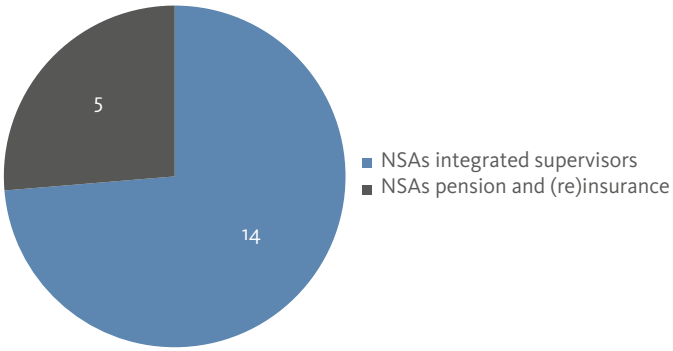
2.4.2 RISKS AND SUPERVISORY EXPERIENCE ASSOCIATED TO CLOUD OUTSOURCING

Information on the key risks, concerns and experience highlighted by NSAs associated to the cloud computing has been gathered from NSAs through:

- a questionnaire on specific cloud outsourcing aspects (definitions and national guidance) as source for supervisory authorities concerns and experience;
- a survey to assess whether risks arising from the use of cloud computing are different for banking and (re) insurance undertakings.

Particularly, the purpose of the survey is to assess whether risks arising from the use of cloud computing are different for banking and (re)insurance undertakings. For this reason, it is built upon the following key underlying question: "are there (re)insurance sector specific risks associated to cloud computing?"

Annex 3 contains the list of the 20 NSAs from 19 jurisdictions that have answered to the survey (UK PRA and FCA have provided a joint reply). From a country perspective, as reported within the chart below, 14 NSAs are integrated supervisors and 5 NSAs do not supervise the banking sector (focused on pension and (re)insurance undertakings).



The assessment here follows the structure of the survey, the supervisory concerns and experiences are highlighted for each relevant area, as applicable.

The survey is divided in seven sections aimed at covering the main risk categories that can arise from the usage of cloud computing.[33]

A) Governance risks

B) Business continuity risks

C) Legal risks

D) Political and compliance limitation risks

E) Concentration risks

F) Data and information security risks

G) Other operational risks

Each section is divided in specific attributes to cover all the risk *spectrum* (all of the attributes are addressed within the EBA Recommendations). NSAs have been requested to highlight whether the risk attribute was relevant for a (re)insurance undertaking, giving further possibility to share their comments.

33 Key source for defining the risk categories are the EBA Recommendations. For this reason, all the risk categories are considered applicable to the banking industry. At Annex 6 it is reported a reconciliation table between the risks categories and the paragraph of the EBA Recommen-dations where those risks are addressed.

A) Governance risks

For the purpose of the survey, the governance risks are arising from:

(i) Lack of a proper incident management process for outsourced services

(ii) Inadequate performance management of the services outsourced to the cloud

(iii) Lack of a proper data and information governance management process

(iv) Inadequate definition of roles and responsibilities between the cloud provider and the supervised undertaking in relation to, for example: (a) IT asset management; (b) User and access management; (c) System and application access; (d) IT security and cybersecurity; (e) subcontract management; (f) transition phase; (g) exit strategies

(v) Poor knowledge, steering and governance of the underlying processes and activities outsourced to the cloud by the supervised undertaking

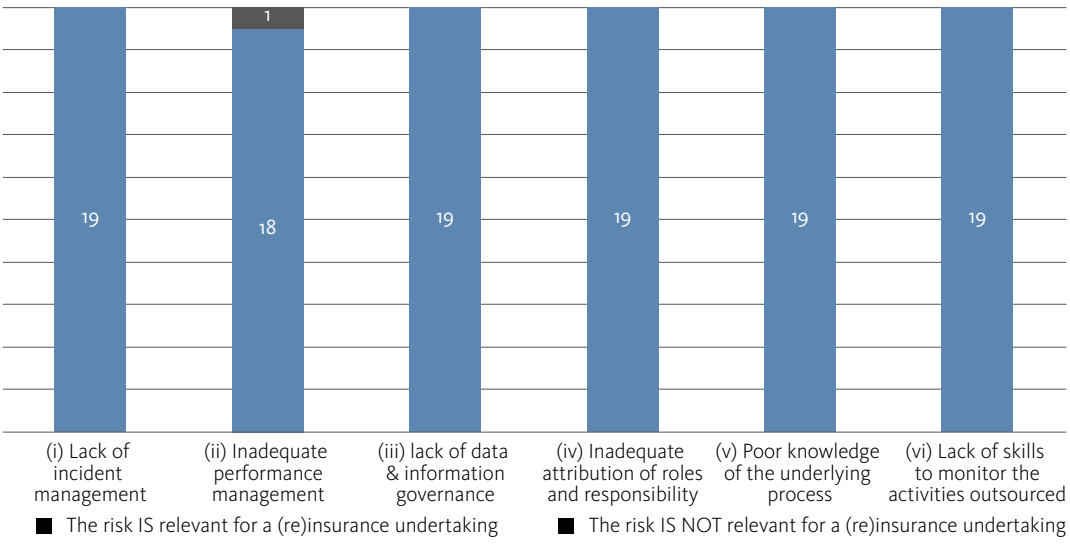
(vi) Lack of skills and resources (of the supervised entity) to monitor the outsourced services / infrastructure outsourced to the cloud

The key underlying risk associated with Governance risks is the risk of losing control, oversight and a comprehensive view over the activities outsourced to the cloud[34]. It is important to underline that, as stated by art. 49 (1) of the Directive, the responsibility of outsourced activities must stay within the (re)insurance undertaking.

The chart below represents the number of NSAs that consider each Governance risk, as defined above, relevant for a (re)insurance undertakings.

Other significant governance related risks (non (re)insurance specific) highlighted by the NSAs are:

- Lack of skills and resources within the supervisor to identify and monitor the above-mentioned risks.
- Loss of business reputation due to other tenants´ activities.
- Lack of governance and structure of the cloud provider (e.g. inappropriate structure of the service provider's information security organisation, insufficient segregation of duties; lacking independent audit of the cloud provider, i.e. security audits, vulnerability



34 As further remark on this point, one NSA commented "We see particularly risks in managing complex entities and long value chains. In particular when a service is built by using several sub-contractors and outsourcing partners. The risk is that no-one has a clear picture of the service entity and its risk management, in particular related questions on continuity and incident management" and another NSA highlighted "Risks arising from losing the big picture: strategic risks (IT architecture impact on or impacted by changes in undertaking's critical success factors)?"

assessments, penetration tests; insufficient risk management of human resources, i.e. vetting, disciplinary actions, security awareness trainings; poor risk management, i.e. ineffective identification, assessment and mitigation of cloud risks; insufficient assurance on the effectiveness of the cloud provider's risk mitigation measures pertaining to the control environment of the services provided).

- Risk of accessing confidential information.
- Lack of adequate risk assessment process and challenge when making decisions to outsource to the cloud.

Moreover, specific guidance on local governance and IT systems requirements was published by AT[35], IT[36] and DE.[37]

As a general recommendation, having sound data governance is crucial in using cloud services appropriately, given that data and system security[38] are paramount. Undertakings also benefit from the encryption of the data outsourced to the cloud.

As a sound data governance practice, it is crucial to classify the data managed. In this regard, certain financial institutions who do not have proper data classification processes in place, find it difficult to assess the materiality of the outsourcing as they do not put a "value" on the data stored with the outsource partner should there be a data breach or a data loss.

TAKEAWAYS: the governance risks associated with cloud computing applicable for (re)insurance undertakings are aligned with those for banking players.

35 Please, see https://www.fma.gv.at/en/fma/fma-guides/

36 The current regulation on governance and IT systems requires in case of outsourcing - including in cloud - the same controls and risks assessment procedures as in case of internal systems

37 For undertakings supervised by the BaFin: implementation of the BaFin circular concerning supervisory requirements for IT in the insurance sector (Versicherungaufsichtliche Anforderungen an die IT: VAIT; Link)

38 For example, With respect to outsourced cloud computing services, the ACPR published a number of data and systems security best practices in July 2013, with which institutions are expected to comply, as well as with the EBA recommendations issued in December 2017.

B) Business Continuity risks

For the purpose of the survey, the business continuity risk is defined as the "risk of losses (e.g. fines, lawsuits, and contractual penalties), reputational damages (e.g. impacts on brand reputation) or impact on perspective revenues due to one or more incidents[39] affecting the services / infrastructure outsourced to the cloud".

All the NSAs that answered the survey consider the business continuity risks, as defined above, relevant for a (re) insurance undertakings.

Supervisory concerns and experience

An NSA reported a business continuity incident (IT incident) related to cloud outsourcing issues: service interruption even though business continuity plans were in place.

TAKEAWAYS: the business continuity risks associated to cloud computing applicable for (re) insurance undertakings are aligned with those for banking players.

C) Legal risks

For the purpose of the survey, the legal risks are arising from the contractual agreement between the (re)insurance undertaking and the cloud provider and are related to:

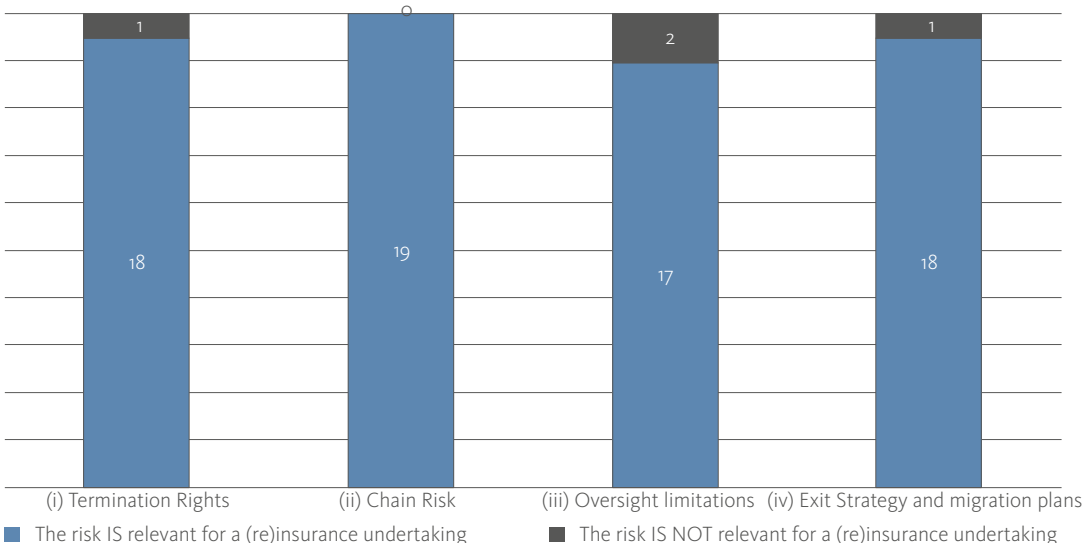
(i) Termination rights in case of, for example: breach of contractual agreements, not notified sub-contracting or other relevant issues;

(ii) Management of sub-contracting issues (chain risks);

(iii) Oversight limitations, such as: limitations of the audit rights for (a) statutory auditors (b) the undertaking (c) any third party appointed for that purpose (d) competent authority.

39 In this context incident is defined as any situation that leads to, a disruption, loss, emergency or crisis.

A situation can affect either the cloud service provider, the supervised entity, the technological chain, or the supply chain



(iv) Exit strategies and migration plans.

The chart above represents the number of NSAs that consider each of the above risks relevant for a (re)insurance undertakings

With reference to the "(iii) oversight limitations" two NSAs made reference to the applicable law (i.e. outsourcing contracts cannot limit rights for supervisors and should provide for audit rights to the undertaking) as their reason to answer "NO" to this question.

Other significant legal related risks highlighted by the NSAs are:

- When considering a consumer complaint regarding breach of data protection, it shall be clear, for the (re)insurance companies, whether or not they have the right of some form of redress against the cloud services provider. Also copyright could be one of the main legal challenges when it comes to cloud computing in general.
- Changing regulations applicable to entities or cloud provider.
- For S-II undertakings: Inadequate implementation of the total requirements of Art. 274 (3) and (4) of the Delegated Regulations.
- Risk of supervisor not being able to access the undertakings data, i.e. cloud provider not granting access when needed. Risk of complications because of legal jurisdiction.

Supervisory concerns and experience on undertaking's audit rights within the agreement between the undertakings and the cloud service providers. After the publication of the EBA Recommendations and due to the increasing use of cloud providers by financial institutions, some good practices have emerged (e.g. pooled audit on two cloud providers performed in an EU jurisdiction by several financial firms of the banking sector).

According to the questionnaire results, in the (re)insurance market there is not a significant track record of inspections carried out on cloud service providers by (re) insurance and reinsurance undertakings.[40]

TAKEAWAYS: the legal risks associated with cloud computing applicable for (re)insurance undertakings are aligned with those for banking players.

For (re)insurance undertakings, it is also crucial to monitor the application of the applicable law (in particular the Art. 274 (3) and (4) of the Delegated Regulations)

40 In one European jurisdiction the undertaking start to make use of their contractual clauses according to audit rights. A few inspections on national service providers have been rounded by the NSA.

D) Political and compliance limitation risks

For the purpose of the survey, the political and compliance limitation risks might arise from contractual agreements between the (re)insurance undertaking and the cloud provider (mainly outside the EEA) due to:

(i) applicable law governing outsourcing contracts;

(ii) possible data protection risks;

(iii) law enforcement provisions including insolvency law that would apply in case of cloud provider failure;

(iv) risks to prevent effective supervision, such as execution of audit rights by: (a) statutory auditors (b) the undertaking (c) any third party appointed for that purpose (d) competent authority.

The chart below represents the number of NSAs that consider each of the above risk relevant for a (re)insurance undertakings.

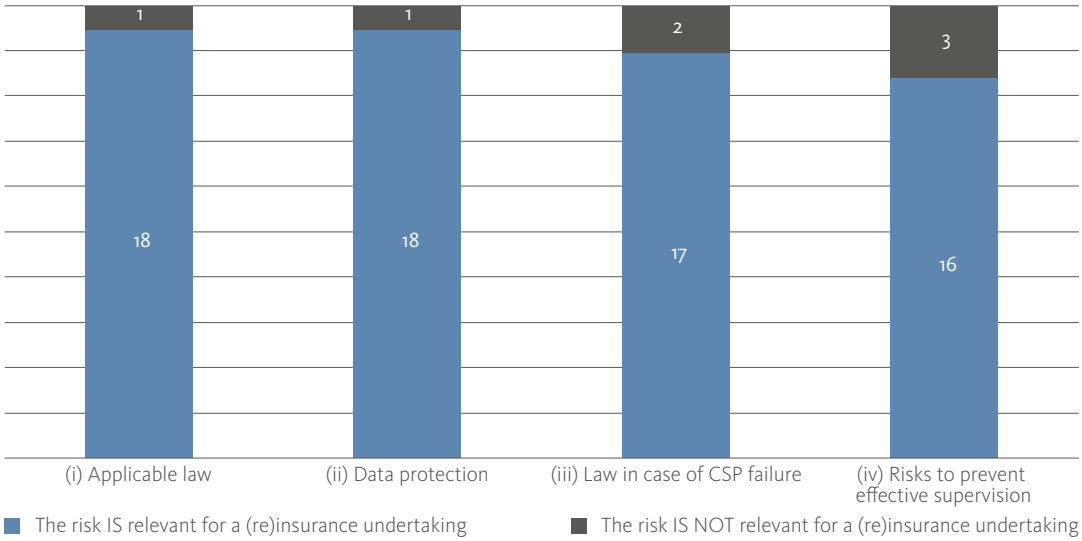
A NSA replied "NO" to all of the questions of the section as to best of their knowledge most (re)insurance undertakings within their market use only EEA based clouds.

With reference to the "(iv) risk to prevent effective supervision", in addition to the NSA reported above, another one answered "NO", and made reference to the applicable law (i.e. Outsourcing contracts cannot limit rights for supervisors and should provide for audit rights to the undertaking).

A NSA has not answered questions related to "(iii) law in case of cloud provider failure" and "(iv) risk to prevent effective supervision". For clarity of representation, in the chart above these answers are reported as if this NSA has answered "NO" to the question.

Other significant political and compliance limitations risks (mostly **not** (re)insurance specific) highlighted by the NSAs included:

- The lack of information about the applicable law in case of any cross-border, legal disputes may lead to confusion in the (re)insurance companies.
- If the (re)insurance undertaking that outsource to the cloud is owned by a larger non-EEA based group, there might be legal issues, but none that we are currently aware of.
- In case sensitive health data are stored and managed on the cloud (regardless whether in EAA or outside), this could raise an issue more specific to (re)insurance. For example, in an EU country there is a dedicated status to the service providers that provide hosting services for these kind of data (but not under the insurance supervisory authority remit, rather Health Ministry). Moreover sometimes insurers can use cloud services going further than data hosting, and there could be further issues regarding the use of some sensitive data for pricing differing from what we get in the banking sector (even if some similarities with credit scoring).



- The cloud provider or its sub-contractors may be obliged to provide data to authorities based on local regulations (maybe even without providing notifications to their clients). This risk is not (re)insurance specific.
- National (non-EU) legislation giving intelligence agencies the right to access data, even when hosted within the EU[41], for instance the United States intelligence agencies can request reporting of data to US cloud providers regardless of their location (US of EU) of the data (Cloud act, Patriot act).

Supervisory experience on supervisor's audit rights (including physical access) within the agreement between the undertakings and the cloud service providers

- Also in this case some good practices have emerged (e.g. relying on external certifications and cloud provider's audit reports). However, there is no homogeneity of approaches for relying on external certifications and cloud provider's audit reports and a limited number of inspections have been carried out on cloud service providers by (re)insurance and reinsurance NSAs.

TAKEAWAYS: the political and compliance limitations risks associated to cloud computing applicable for (re)insurance undertakings are aligned with those for banking players.

For (re)insurance undertakings, it is important to highlight that the customer health data stored or managed with cloud computing resources must be treated with particular care (e.g. in case of outsourcing of activities or processes related to those data, the NSA must be always informed)

E) Concentration risk

For the purpose of the survey, the concentration risk is associated with the risk of operational lock-in (i.e. difficult to find a different cloud service provider).[42]

All the NSAs that answered the survey consider concentration risks, as defined above, relevant for a (re)insurance undertakings. Moreover, the NSAs highlighted the following aspects of the concentration risk (mostly **not** (re) insurance specific):

- In case the cloud service provider no longer meets their requirements, (re)insurance undertakings should have exit strategies.
- In case an (re)insurance undertaking is providing coverage to the cloud provider (e.g. cyber insurance or even property for the cloud provider datacentres), it could undergo, at the same time, operational risk on its essential service provider and an underwriting risk because it bears the liability risk of this service provider towards other clients. This possibility might not be totally accounted for in the standard formula.
- In our view "operational lock-in" (or vendor lock-in) is less significant from a concentration risk perspective. By concentration risk we think of a situation when a small number of big Cloud Providers have many customers from the (re)insurance sector. In this case the failure of one cloud provider may disrupt the operations of a significant number of (re)insurance undertakings, thereby posing a concentration risk.
- The risk of malfunction or other operation failure of the cloud service provider, when a large part of the (re)insurance market is using their services. E.g. if Solvency Tool would fail, 3/4 of the domestic (re)insurance market of an EU country would be affected.
- Concentration risks anywhere in the IT production (one provider supplying same service to multiple undertakings).

As a general comment, the risk of concentration of sensitive data / process management within just a few cloud service providers is perceived by many NSAs as an issue for the future.

TAKEAWAYS: the concentration risk associated to cloud computing applicable for (re)insurance undertakings are aligned with those for banking players.

In case a (re)insurance undertaking is provider of (re)insurance coverage to key risks of the cloud provider (e.g. cyber, property, fire, etc.), this aspect shall be taken into account during the outsourcing evaluation phase.

41 Entering into an agreement with a CSP obligated to follow non-EU legislation (i.e. obligated to give non-EU intelligence agencies access to the hosted data) shall be considered as: (1) a potential risk? (2) an incurred risk? (a conscious and deliberate course of conduct with knowledge of the circumstances)

42 In the IaaS market at global level, the four biggest cloud service providers represents nearly three quarters (i.e. ~73%) of the market. à LINK

F) Data and information security risks

For the purpose of the survey, the data and information security risks are the risk of losses (e.g. fines, lawsuits, and contractual penalties), reputational damages (e.g. impacts on brand reputation) or impact on perspective revenues due to:

(i) With reference to the supervised entity, inadequate: (a) data classification and assessment; (b) identification of data protection measures (e.g. encryption, integrity, traceability); (c) back-up requirements/management; (d) IT security and cybersecurity processes.

(ii) With reference to the cloud service providers: (a) poor data and information management (i.e. data confidentiality and information integrity and availability); (b) IT security incidents (c) poor service performance (d) back-up management; (e) IT security and cybersecurity; (f) other operational risks (e.g. data lock-in).

All the NSAs that answered the survey consider the data and information security risks, as defined above, relevant for a (re)insurance undertaking. Moreover, the NSAs highlighted the following aspects of data and information security risks. Most of them are **not** (re)insurance specific and consists of better specification of the risk categories listed within the survey.

- Unauthorized access to data and exposition of personal data due to breach in cybersecurity.
- Insecure or insufficient data deletion on the cloud provider side (data would be available when it shouldn´t be)
- Processing of business transactions without human interaction ("shadow processing") for (re)insurance specific activities, e.g. claims processing or pricing
- Cloud providers that also offer insurance (GAFA) could potentially use customer or other kinds of data of (re)insurance undertakings for themselves
- Risks related to data in transit, e.g. poor authentication of the assets and users involved in communication; insufficient availability of network connectivity or bandwidth for normal operation.
- Risks related to data stored, e.g. poor access rights management by the cloud provider; unsafe deletion of stored data, including backups and archives; unsafe destruction of data storage devices and media during disposal; data backups not stored independently by the customer for critical functionalities or systems.
- Risks related to data protection, e.g. different regulatory requirements on data protection for the customer and the cloud provider, resulting in different data protection commitments, practices and data reporting obligations.
- When undertakings use their own encryption on data stored in cloud solutions there is the risk of the supervisor not being able to utilize the data even though access is not restricted by the cloud solution provider.
- The communications operator can be also a risk, because it could also fail.

TAKEAWAYS: the data and information security risk associated to cloud computing applicable for (re)insurance undertakings are aligned with those for banking players.

G) Other operational risks

NSAs have highlighted the other operational risks reported below within the survey. Most of them are not (re)insurance specific and consist of better specification of the risk categories listed within the survey.

- Data availability and business continuity - a major risk to business continuity in the cloud computing is a possible loss of internet connectivity. Also companies should have their own "disaster recovery" plans in order to respond quickly and accordingly in case any technical problems occur. However, even if they do have such plans, they are invariably connected with the "disaster recovery" plans of the cloud services provider. In the case of lack of different providers of cloud services of the market, this presents new heights for the concentration risk.
- Network issues (prerequisite of a reliable cloud solution is a solid and redundant Network connection)
- Business continuity risks, for example in the case of power outage, network outage etc.
- Operational risks may also arise when cloud security, operations and development processes are ineffective or not followed.
  - Risks involved in cloud security and operations management (e.g. ineffective security architec-

ture planning, ineffective change, version and configuration management, ineffective process for correcting security vulnerabilities, ineffective protection against malicious codes, insufficient monitoring and logging of operations, ineffective security logging and monitoring).

- Risks involved in the development processes of the cloud services provided (e.g. documented development guidelines and methodologies are not applied, security requirements are not identified in developments, separate development, test and production environments are not utilised, no security and penetration tests performed prior to going live, and at least annually during live operation, no quality assurance exercised on developments performed by sub-contractors).

› Insolvency of cloud provider and cyber-attack on cloud provider

› Small (re)insurance undertakings have less leverage when negotiating with big suppliers. Legal risks above are augmented if small actors are "forced" to accept standard agreements.

› Operational risks could also arise through a wrong management of the outsourcing chains (incl. cloud outsourcing through parent company).

The Solvency II legal framework states that an insurer is responsible for fulfilling the legal requirements on outsourcing regardless if the outsourcing is intra-group or the number of sub delegations (Delegated Acts art. 274(2) and EIOPA System of Governance guidelines nr. 62).

- Outsourcing chains (including on cloud) are becoming longer due to the strategic focus on core competencies of value chain actors (i.e. regulated undertakings and service providers). To properly manage the outsourcing chains (including on cloud) a sound governance system should be in place. Moreover, it has to be noted that longer chains increase also the risk of concentration in service providers.

- In case of multinational groups, a cloud outsourcing agreement could be negotiated by the parent company (or by the group internal IT service providers) for services that are used by multiple group entities. This might happen for multiple reasons (e.g. cost efficiency, IT strategy of the group, IT deployment model of the group, etc.).

When this happen, normally, both the parent company and the group subsidiaries have to notify or gain a regulatory approval from the use of cloud by each of its supervisors. This could result in higher costs for the group, a longer time to market in deploying the solution and/or risk of inconsistency in the regulatory approach.

TAKEAWAYS:

- The impact of cloud computing on the (re)insurance market is assessed differently among jurisdictions;
- The EBA Recommendations are becoming the market standard contributing to solve some issues (i.e. audit rights and practices);
- Due to the complexity and the high level of technicality of the subject, some jurisdictions[43] have planned to issue (or already issued) national guidance directly applicable to the (re)insurance market on cloud outsourcing;
- From a legal point of view cloud computing falls within the outsourcing provisions. In light of this, the financial institutions are required to classify the cloud services they receive as "critical or important". The most common approach within the (re)insurance industry is to classify cloud computing on a case-by-case – similarly to the other services – on the basis of the service/process/activity/data outsourced[44]
- Some issues related to risks that may arise on cloud computing have been highlighted as relevant and are addressed within the EBA Recommendations (i.e. Auditability of cloud services (internal audit, external audit, regulators); Data management and encryption, lock-in effect from cloud providers (termination rights); sound management of the outsourcing chains (incl. cloud outsourcing through parent company); risk concentration)
- The risks arising from the usage of cloud computing by (re)insurance undertakings appear to be, generally, aligned to the risks bear by the banking players with few minor (re)insurance specificities.

43 CZ, DE, FI, SE, UK-FCA, PL, FR

44 This approach appears to be coherent with the principle based guidance on how to classify the services as "critical" or "important" provided by the EBA Guideline on Outsourcing Arrangements.

2.5. SELECTED EXAMPLES ON CLOUD OUTSOURCING PRACTICES

Within this section are reported some real examples of cloud outsourcing using within the financial sector, highlighting the differences among the (re)insurance market and the others and on the practices adopted by incumbent and new players.

Examples include:

Industry	Country	Player	Description
Banking	DE	New player	Retail banking provider with IT systems fully developed in cloud
Banking	NL	New player	Small credit institution with IT systems fully developed in cloud
Insurance	DE	New player	Non-life insurance company with IT systems fully developed in cloud
Banking and Insurance Group	BE, CZ, HU, IE, SK	Incumbent	Cloud collaboration tool (e-mail and office package. Microsoft 365)
Insurance	ES	Incumbent	Use of cloud to perform the monthly solvency check calculation and to have a flexible development and release environment
Insurance	FR	Incumbent	Branch of a big insurance group with IT systems fully developed in cloud
Payment	FI	New player	Entity which is a technical provider for a Payment institution, that is in the process of applying its own payment institution licence. Their solution is based purely on cloud

3. SUMMARY OF KEY TAKEAWAYS AND EIOPA'S ANSWER TO THE EUROPEAN COMMISSION

The key takeaways of the analysis carried out and described within this document are the following:

(i) cloud computing is mostly used extensively by newcomers, by a niche of the market and by larger undertakings mostly for non-critical function. However, as part of their wider digital transformation strategies many European large (re)insurers are expanding their use of the cloud;

(ii) the current Regulatory framework of Solvency II (level 1 and level 2) appears to be sound to discipline the outsourcing to the cloud by the current outsourcing provisions (Articles 38 and 49 of the Directive and Article 274 of the Delegated Regulations)[45];

(iii) cloud computing is a fast developing service so in order for its regulation to be efficient it should be principle-based rather than attempting at regulating all (re)insurance-related aspects of it;

(iv) cloud computing services used by (re)insurance undertakings are aligned to the one used by banking sector. The risks arising from the usage of cloud computing by (re)insurance undertakings appear to be, generally, aligned to the risks bear by the banking players with few minor (re) insurance specificities;

(v) both banking and (re)insurance regulations discipline cloud computing by their current outsourcing provisions. Under these, banking and (re)insurance institutions are required to classify whether the cloud services they receive are „critical or important". The most common approach is to classify cloud computing on a case-by-case approach – similarly to the other services – on the basis of the service / process / activity / data outsourced;

(vi) the impact of cloud computing on the (re)insurance market is assessed differently among jurisdictions: due to the complexity and the high level of technicality of the subject, some jurisdictions[46] have planned to issue (or already issued) national guidance directly applicable to the (re)insurance market on cloud outsourcing;

(vii) from the gap analysis carried out, the EBA Recommendations are more specific on the subject (e.g. the specific requirements to build a register of all the cloud service providers) and, being built on shared common principles, can be applied to the wide Solvency II regulations on outsourcing, reflecting their status at level 3;

(viii) to provide legal transparency to the market participants (i.e. regulated undertakings and service providers) and to avoid potential regulatory arbitrage, EIOPA should issue guidance on cloud outsourcing aligned with the EBA Recommendations and, where applicable, the EBA Guidelines on outsourcing arrangements with minor amendments.

Having regard to the takeaways of the analysis carried out by its InsurTech Task Force and considering the discussion had with the other ESAs, under the steering of its InsurTech TaskForce, EIOPA will develop its own Guidelines on Cloud Outsourcing.

The intention is that the Guidelines on Cloud Outsourcing (the "guidelines") will be drafted during the first half

45 The Solvency II framework on outsourcing (level 1 and 2) is detailed and clarified by the EIOPA guidelines on system of governance nr. 60-64.

46 CZ, DE, FI, SE, UK-FCA, PL, FR.

of 2019, issued then for consultation and finalised by the end of the year.

During the process of drafting the Guidelines, EIOPA will organize a public roundtable on the use of cloud computing by (re)insurance undertakings. During the roundtable, representative from the (re)insurance industry, cloud service providers and the supervisory community will discuss views and approaches to cloud outsourcing in a Solvency II and post-EBA Recommendations environment.

Furthermore, in order to guarantee a cross-industry harmonization within the European financial sector, EIOPA has agreed with the other two ESAs:

- to continue keeping the fruitful alignment kept so far; and
- to start – in the second part of 2019 – a joint market monitoring activity aimed at developing policy views on how cloud outsourcing in the finance sector should be treated in the future. This should take into account the increasing use of the cloud and the potential for large cloud service providers to be a single point of failure.

ANNEX 1: LIST OF CONSULTED DOCUMENTS

White Papers and standards on cloud computing:

- NIST Cloud Computing Reference Architecture, Recommendations of the National Institute of Standards and Technology, September 2011 LINK
- The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, September 2011 LINK
- The DTCC Moving Financial Market Infrastructure To The Cloud - Realizing the Risk Reduction and Cost Efficiency Vision While Achieving Public Policy Goals, May 2017
- Measuring the economic impact of cloud computing in Europe, A study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte, 2016
- Microsoft Corp., Shared Responsibility for cloud computing, April 2017 LINK
- Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, 2017
- Cloud Security Alliance The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights, 2017
- OECD, Directorate for Science Technology and Industry – Committee on Digital Economy Policy, Cloud Computing: The Concept, Impacts, and the Role of Government Policy, August 19, 2014 LINK
- US Department of the Treasury, A Financial System that creates economic opportunities Nonbank Financials, Fintech and Innovation, July 2018 LINK
- Office of the Superintendent of Financial Institutions (OFSI), Guideline related to Outsourcing of Business Activities, Functions and Processes, last revision in 2009 LINK
- Monetary Authority of Singapore (MSA), Guidelines on outsourcing, July 27, 2016 LINK
- Australian Prudential Regulation Authority (APRA), Information paper on Outsourcing involving shared computing services (including cloud), July 6, 2015 LINK
- Financial Stability Institute (FSI), Regulating and supervising the cloud: emerging prudential approaches for insurance companies, December 5, 2018 LINK

Other relevant documentation issued by European authorities:

- CZ: Official information of the Czech National Bank regarding the pursuit of business in the financial market – cloud computing, 19 August 2016
- DE: Bafin, Circular 02/2017 (VA), Minimum Requirements under Supervisory Law on the System of Governance of Insurance Undertakings
- DE: Bafin, Cloud computing: Compliance with the supervisory requirements regarding rights of information and audit and ability to monitor, 7 May 2018
- EBA Recommendations on cloud outsourcing, December 2017 LINK
- EIOPA: Final report on public consultation No. 14/017 on Guidelines on system of governance

- European Commission, FinTech Action plan: For a more competitive and innovative European financial sector, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, March 8, 2018
- EE: Advisory Guidelines of the Financial Supervision Authority, Outsourcing Requirements for Supervised Entities, 25 October 2006 LINK
- EE: Requirements for the organisation of the information technology and information security of the subject of financial supervision, from 23 January 2017, updated 12 February 2018 LINK
- ES: Guía de seguridad de las tic (CCN-STIC-823), Utilización de servicios en la nube, Esquema Nacional de Seguridad, December 2014
- FI: Regulations and Guidelines 1/2012, Outsourcing in supervised entities belonging to the financial sector, Amended on 14 November 2014. Date of change 23 January 2018. LINK
- FR: ACPR, IT Risk discussion paper, March 2018 LINK
- FR: Recommendations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, CNIL
- FR: ACPR, The risks associated with the cloud computing, July 2013 LINK
- FR: Vocabulaire de l'informatique et de l'internet LINK
- LV: Regulations No 112, Regulations on Information Systems Security, 7 July 2015
- IT: IVASS, Regolamento nr. 38/2018, Regolamento recante disposizioni in materia di sistema di governo societario, 21 July 2018
- PL: KNV, Position of the Office of the Polish Financial Supervision Authority on the use of cloud computing services by supervised entities
- PL: KNV, Guidelines on the Management of Information Technology and ICT Environment Security for Insurance and Reinsurance Undertakings, 14 December 2014
- RO, ASF, Rule no. 4/2018 on the management of operational risks generated by information systems used by authorized / licensed / registered entities, regulated and / or supervised by the Financial Supervisory Authority LINK
- SE: Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer
- UK: FCA, FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third-party IT services, July 2016

ANNEX 2: ITF MEMBERS ANSWERS TO EIOPA QUESTIONNAIRE ON CLOUD OUTSOURCING

Below the list of the ITF Members that have answered to the EIOPA questionnaire on cloud outsourcing:

1. Austria, Austrian Financial Market Authority (FMA)
2. Czech Republic, Czech National Bank
3. Finland, Finanssivalvonta (FIN-FSA)
4. France, Autorite de Controle Prudentiel et de Resolution (ACPR)
5. Germany, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
6. Greece, Bank of Greece
7. Ireland, Central Bank of Ireland (CBI)
8. Italy, Istituto per la Vigilanza sulle Assicurazioni (IVASS)
9. Latvia, Finanšu un Kapitāla Tirgus Komisija (FKTK)
10. the Netherlands, De Nederlandsche Bank (DNB)
11. Poland, Komisja Nadzoru Finansowego (KNF)
12. Portugal, Autoridate de Supervisao (ASF)
13. Romania, Autoritatea de Supraveghere Financiară (ASF)
14. Spain, Ministry of Economy and Competitiveness
15. Sweden, Finansinspektionen
16. United Kingdom, Financial Conduct Authority (FCA)
17. United Kingdom, Prudential Regulation Authority (PRA)

ANNEX 3: ITF MEMBERS ANSWERS TO EIOPA SURVEY ON (RE)INSURANCE SPECIFIC RISKS ASSOCIATED TO CLOUD COMPUTING IN COMPARISON WITH THE BANKING SECTOR

Below the list of the ITF Members that have answered to the EIOPA survey on the (re)insurance specific risks associated to cloud computing in comparison with the banking sector:

1. Austria, Austrian Financial Market Authority (FMA)
2. Bulgaria, Financial Supervision Commission (FSC)
3. Czech Republic, Czech National Bank
4. Estonia, Finantsinspektsioon
5. Finland, Finanssivalvonta (FIN-FSA)
6. France, Autorite de Controle Prudentiel et de Resolution (ACPR)
7. Germany, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
8. Greece, Bank of Greece
9. Hungary, the Central Bank of Hungary (MNB)
10. Iceland, Financial Supervisory Authority
11. Ireland, Central Bank of Ireland (CBI)
12. Italy, Istituto per la Vigilanza sulle Assicurazioni (IVASS)
13. Latvia, Finanšu un Kapitāla Tirgus Komisija (FKTK)
14. Portugal, Autoridate de Supervisao (ASF)
15. Romania, Autoritatea de Supraveghere Financiară (ASF)
16. Slovakia, Národná banka Slovenska (NBS)
17. Spain, Ministry of Economy and Competitiveness
18. Sweden, Finansinspektionen
19. United Kingdom, Financial Conduct Authority (FCA)
20. United Kingdom, Prudential Regulation Authority (PRA)

ANNEX 4: GAP ANALYSIS BETWEEN THE EBA RECOMMENDATIONS AND THE SOLVENCY II PROVISIONS

The table below summarizes a gap analysis between the EBA recommendations and the Solvency II provisions

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Materiality assessment	1. Undertakings should, prior to any outsourcing of their activities, assess which activities should be considered as material. The assessment - for outsourcing to cloud service providers – should mainly take into account all of the following: a) the criticality and inherent risk profile of the activities to be outsourced[47] b) the direct operational impact of outages, and related legal and reputational risks; c) the impact that any disruption of the activity might have on the institution's revenue prospects; d) the potential impact that a confidentiality breach or failure of data integrity could have on the institution and its customers	**Article 49 (2)** Outsourcing of critical or important operational functions or activities shall not be undertaken in such a way as to lead to any of the following: a) materially impairing the quality of the system of governance of the undertaking concerned; b) unduly increasing the operational risk; c) impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations; d) undermining continuous and satisfactory service to policy holders. **Article 274 (3) and (4)** (3) When choosing the service provider referred to in paragraph 1 for any critical or important operational functions or activities, the administrative, management or supervisory body shall ensure that: a) a detailed examination is performed to ensure that the potential service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily, taking into account the undertaking's objectives and needs **Guideline 60** The undertaking should determine and document whether the outsourced function or activity is a critical or important function or activity on the basis of whether this function or activity is essential to the operation of the undertaking as it would be unable to deliver its services to policyholders without the function or activity **Guideline 63** The undertaking that outsources or considers outsourcing should cover in its policy the undertaking's approach and processes for outsourcing from the inception to the end of the contract. This in particular should include: a) the process for determining whether a function or activity is critical or important;	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Duty to adequately inform supervisors	2. Outsourcing institutions should adequately inform the competent authorities of material activities to be outsourced to cloud service providers and in any case make available to the competent authorities the information listed within the Recommendations 3. The competent authority may ask the outsourcing institution for additional information on its risk analysis for the material activities to be outsourced 4. The outsourcing institution should maintain an updated register of information on all its material and non-material activities outsourced to cloud service providers at institution and group level. 5. Detailed list of the information to be contained within the register	**Article 49 (3)** Insurance and reinsurance undertakings shall, in a timely manner, notify the supervisory authorities prior to the outsourcing of critical or important functions or activities as well as of any subsequent material developments with respect to those functions or activities. **Article 274 (1)** Any insurance or reinsurance undertaking which outsources or proposes to outsource functions or insurance or reinsurance activities to a service provider shall establish a written outsourcing policy which takes into account the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented in cases of outsourcing. **Guideline 64** In its written notification to the supervisory authority of any outsourcing of critical or important functions or activities the undertaking should include a description of the scope and the rationale for the outsourcing and the service provider's name. When outsourcing concerns a key function, the information should also include the name of the person in charge of the outsourced function or activities at the service provider.	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed in particular on reporting to competent authorities (the draft EBA guidelines on outsourcing arrangements foresees a common DB format)

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Access and audit rights (for Undertakings)	6. Outsourcing institutions should further ensure that they have in place an agreement in writing with the cloud service provider whereby the latter undertakes the obligation: e) To provide to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor full access to its business premises; f) To confer to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor, unrestricted rights of inspection and auditing related to the outsourced services (right of audit). 7. The effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements. 8. The outsourcing institution should exercise its rights to audit and access in a risk-based manner. Where an outsourcing institution does not employ its own audit resources, it should consider using at least one of the following tools: (a) Pooled Audits[48]; (b) third party certifications and third-party or internal audit reports made available by the cloud service provider according to certain provisions[49]. 9. Considering that cloud solutions have a high level of technical complexity, the outsourcing institution should verify that the staff performing the audit – being its internal auditors or the pool of auditors acting on its behalf, or the cloud service provider's appointed auditors appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the right skills and knowledge to perform effective and relevant audits and/or assessments of cloud solutions	**Article 38** Member States shall ensure that insurance and reinsurance undertakings which outsource a function or an insurance or reinsurance activity take the necessary steps to ensure that the following conditions are satisfied: b) the insurance and reinsurance undertakings, their auditors and the supervisory authorities must have effective access to data related to the outsourced functions or activities; **Article 274 (4)** The written agreement referred to in paragraph 3 (c) to be concluded between the insurance or reinsurance undertaking and the service provider shall in particular clearly state all of the following requirements: h) that the insurance or reinsurance undertaking, its external auditor and the supervisory authority have effective access to all information relating to the outsourced functions and activities including carrying out on-site inspections of the business premises of the service provider	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed and contain specific provisions that enable the undertaking to use the following audit tools

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Access and audit rights (for NCAs)	10. Outsourcing institutions should ensure that they have in place an agreement in writing with the cloud service provider whereby the latter undertakes the obligation: a) to provide to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) full access to the cloud service provider's business premises (head offices and operations centres), including the full range of devices, systems, networks and data used for providing the services to the outsourcing institution (right of access); b) to confer to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) unrestricted rights of inspection and auditing related to the outsourced services (right of audit).	**Article 38** Without prejudice to Article 49, Member States shall ensure that insurance and reinsurance undertakings which outsource a function or an insurance or reinsurance activity take the necessary steps to ensure that the following conditions are satisfied: a) the service provider must cooperate with the supervisory authorities of the insurance and reinsurance undertaking in connection with the outsourced function or activity; b) the insurance and reinsurance undertakings, their auditors and the supervisory authorities must have effective access to data related to the outsourced functions or activities; c) the supervisory authorities must have effective access to the business premises of the service provider and must be able to exercise those rights of access. 2. The Member State where the service provider is located shall permit the supervisory authorities of the insurance or reinsurance undertaking to carry out themselves, or through the intermediary of persons they appoint for that purpose, on-site inspections at the premises of the service provider.	Topic already covered by the Solvency II-framework
In particular for the right of access	14. The agreement between the undertaking and the cloud service provider should have the following provisions: (a) prior notification to the cloud service provider unless due to emergency or crisis (b) The cloud service provider is required to fully cooperate in connection with the on-site visit	**Article 49 (2-c)** Please see above **Article 274 (4-h)** Please see above	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Security of data and systems	15. The outsourcing contract should oblige the outsourcing service provider to protect the confidentiality of the information transmitted by the financial institution. 16. The institution should perform, prior to outsourcing and for the purpose of informing the relevant decision, at least the following: a) classify its activities, processes and related data and systems as to the sensitivity and required protection; b) conduct a thorough risk-based selection of the activities, processes and related data and systems which are under consideration to be outsourced to a cloud computing solution; c) define and decide on an appropriate level of protection of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended cloud outsourcing. Institutions should also consider specific measures where necessary for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture 17. The above 16(c) should be set out within the contract in writing	**Article 274 (3)** When choosing the service provider referred to in paragraph 1 for any critical or important operational functions or activities, the administrative, management or supervisory body shall ensure that: e) the outsourcing does not entail the breaching of any law in particular with regard to rules on data protection; f) the service provider is subject to the same provisions on the safety and confidentiality of information relating to the insurance or reinsurance undertaking or to its policyholders or beneficiaries that are applicable to the insurance or reinsurance undertaking **Article 274 (4)** The written agreement to be concluded between the insurance or reinsurance undertaking and the service provider shall in particular clearly state all of the following requirements: (b) the service provider's commitment to comply with all applicable laws, regulatory requirements and guidelines as well as policies approved by the insurance or reinsurance undertaking and to cooperate with the undertaking's supervisory authority with regard to the outsourced function or activity; (f) that the insurance or reinsurance undertaking reserves the right to be informed about the outsourced functions and activities and their performance by the services provider as well as a right to issue general guidelines and individual instructions at the address of the service provider, as to what has to be taken into account when performing the outsourced functions or activities; (g) that the service provider shall protect any confidential information relating to the insurance or reinsurance undertaking and its policyholders, beneficiaries, employees, contracting parties and all other persons	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed
Location of data and data Processing	19. Special care for non EEA service providers (incl. wider political and security stability of the jurisdictions, laws in force, etc.) 20. Risk-based approach to ensure risks are kept within acceptable limits	**Article 274 (3-e/f)** Please see above **Article 274 (4-b/f/g)** Please see above	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Chain outsourcing	21. The outsourcing institution should agree to chain outsourcing only if the sub-contractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider. Furthermore, the outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement 22. The outsourcing agreement between the outsourcing institution and the cloud service provider should specify any types of activities that are excluded from potential subcontracting. The cloud service provider retains full responsibility for and oversight of those services that it has subcontracted. 23. obligation for the cloud service provider to inform the outsourcing institution of any planned significant changes to the sub-contractors or the subcontracted services named in the initial agreement that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement 24. The outsourcing institution should have the right to terminate the contract.in case the change of sub-contractor have adverse effects risk assessment of the agreed services 25. The outsourcing institution should review and monitor the performance of the overall service on an ongoing basis, regardless of whether it is provided by the cloud service provider or its sub-contractors.	**Article 274 (4)** The written agreement referred to be concluded between the insurance or reinsurance undertaking and the service provider shall in particular clearly state all of the following requirements: (c) the service provider's obligation to disclose any development which may have a material impact on its ability to carry out the outsourced functions and activities effectively and in compliance with applicable laws and regulatory requirements; (k) the terms and conditions, where applicable, under which the service provider may sub-outsource any of the outsourced functions and activities; (l) that the service provider's duties and responsibilities deriving from its agreement with the insurance or reinsurance undertaking shall remain unaffected by any sub-outsourcing taking place according to point (k).	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed in particular for the explicit need for the outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities

Item	EBA Recommendations key Features	Solvency II provisions	GAP analysis results
Contingency plan and exit strategy	26. Outsourcing institution to plan and implement arrangements to maintain the continuity of its business including contingency planning, a clearly defined exit strategy and termination clause. 27. An outsourcing institution should also ensure that it is able to exit cloud outsourcing arrangements, if necessary, without undue disruption to its provision of services or adverse effects on its compliance with the regulatory regime and without detriment to the continuity and quality of its provision of services to clients. 28. When developing exit strategies, an outsourcing institution should consider the following: (a) Key Risk Indicators within SLAs; (b) performance of a business impact analysis (c) assign roles and responsibilities to manage exit plans and transition activities (d) define success criteria for the transition 29. The outsourcing institution should include indicators that can trigger the exit plan in its ongoing service monitoring and oversight of the services provided by the cloud service provider.	**Article 274 (4)** The written agreement referred to be concluded between the insurance or reinsurance undertaking and the service provider shall in particular clearly state all of the following requirements: (d) a notice period for the termination of the contract by the service provider which is long enough to enable the insurance or reinsurance undertaking to find an alternative solution; (e) that the insurance or reinsurance undertaking is able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of services to policyholders; **Article 274 (5)** (d) ensure that the service provider has adequate contingency plans in place to deal with emergency situations or business disruptions and periodically tests backup facilities where necessary, taking into account the outsourced functions and activities. Guideline 63 The undertaking that outsources or considers outsourcing should cover in its policy the undertaking's approach and processes for outsourcing from the inception to the end of the contract. This in particular should include: b) how a service provider of suitable quality is selected and how and how often its performance and results are assessed; d) business contingency plans, including exit strategies for outsourced critical or important functions or activities	Topic already covered by the Solvency II-framework. The EBA recommendations are more specific and detailed particularly requiring the presence of KRIs and SLAs

47 I.e. are they activities that are critical to the business continuity/viability of the institution and its obligations to customers

48 Pooled audits organised jointly with other clients of the same cloud service provider, and performed by these clients or by a third party appointed by them, in order to use audit resources more efficiently and to decrease the organisational burden on both the clients and the cloud service provider.

49 (i) The outsourcing institution ensures that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and the controls identified as key by the outsourcing institution. (ii) The outsourcing institution thoroughly assesses the content of the certifications or audit reports on an ongoing basis, and in particular ensures that key controls are still covered in future versions of an audit report and verifies that the certification or audit report is not obsolete. (iii) The outsourcing institution is satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file). (iv) The certifications are issued and the audits are performed against widely recognised standards and include a test of the operational effectiveness of the key controls in place. (v) The outsourcing institution has the contractual right to request the expansion of scope of the certifications or audit reports to some systems and/or controls that are relevant. The number and frequency of such requests for scope modification should be reasonable, and legitimate from a risk management perspective.

ANNEX 5: IS THE ENCRYPTION OF ALL THE DATA STORED WITHIN THE CLOUD A SOLUTION?

"Below the answer received on the question: "Can requiring the financial institution to encrypt all the data outsourced to the cloud be a solution?"

Cloud data encryption is a very effective tool for mitigating the risks of this outsourcing. On the other hand, encrypting all of the data could lead to technological limitations in the use of some information systems and the removal of these difficulties could be costly. It can be assumed that data of different importance will be processed and stored in the cloud. Institutions should take into account the risks of cloud implementation and suggest how to adequately protect data. In particular, it is the right choice for encryption technology for data in transit, data in memory and data at rest. Institutions should also consider risks arising from the management of encryption keys

This could give some more stability to data security issues. However, encryption does usually not give 100% security guarantee. Instead, insurers should be encouraged to consider these issues in their risk analysis adequately and using current data security standards.

Yes, especially for sensitive (i.e. health insurance data) or confidential data. Encryption in itself is no guarantee, but it will help mitigate the cloud outsourcing risks

It depends on the confidentiality or otherwise relevance of data. Full encryption could be helpful but costly and not efficient. Responsibility for data management should be clearly declared with explicit ownership and technical solutions.

I would expect that big cloud service providers offer encryption solutions by default, linked to access rights. Encryption can help protecting access to data, however without additional technical information regarding the actual cloud service providers, it is difficult to provide a definitive answer.

Encryption is a good part of general cyber-hygiene and something which institutions would be routinely expected to do under the shared responsibility model. However, it is not a panacea and needs to be accompanied by other risk identification, management and mitigation practices by insurers

ANNEX 6: RECONCILIATION BETWEEN THE CLOUD SURVEY RISK CATEGORIES AND THE EBA RECOMMENDATIONS

The table below provides a mapping between the paragraphs of the EBA Recommendations and the risk categories used within the survey shared among the ITF members to assess whether risks arising from the use of cloud computing are different for banking and (re)insurance undertakings**.**

A. Governance risks	**EBA Recom. reference [par. #]**
Risks arising from:	
Lack of a proper incident management process for outsourced services	[4.5]
Inadequate performance management of the services outsourced to the cloud	[4.5 & 4.8]
Lack of a proper data and information governance management process	[4.5]
Inadequate definition of roles and responsibilities between the cloud provider and the supervised undertaking in relation to, for example: (i) IT asset management; (ii) User and access management; (iii) System and application access (iv) IT security and cybersecurity; (v) subcontract management; (vi) transition phase; (vii) exit strategies	[4.5, 4.7 & 4.8]
Poor knowledge, steering and governance of the underlying processes and activities outsourced to the cloud by the supervised undertaking	[4.1]
Lack of skills and resources (of the supervised entity) to monitor the outsourced services / infrastructure outsourced to the cloud	[4.2]
B. Business continuity risk	**EBA Recom. reference [par. #]**
Risk of losses (e.g. fines, lawsuits, and contractual penalties), reputational damages (e.g. impacts on brand reputation) or impact on perspective revenues due to one or more incidents* affecting the services / infrastructure outsourced to the cloud. * In this context incident is defined as any situation that leads to, a disruption, loss, emergency or crisis. A situation can affect either the cloud service provider, the supervised entity, the technological chain, or the supply chain.	[4.1, 4.5 & 4.8]
C. Legal risks	**EBA Recom. reference [par. #]**
Risks arising from the contractual agreement with the cloud service provider related to:	
Termination rights in case of, for example: breach of contractual agreements, not notified sub-contracting or other relevant issues	[4.1 & 4.8]

Management of sub-contracting issues (chain risks);	[4.7]
Oversight limitations, such as: limitations of the audit rights for (i) statutory auditors (ii) the undertaking (iii) any third party appointed for that purpose (iv) competent authority	[4.3]
Exit strategies and migration plans	[4.8]
D. Political and compliance limitation risks	**EBA Recom. reference [par. #]**
Risks arising from a contractual agreement (mainly) outside the EEA for:	
applicable law governing outsourcing contracts	[4.2 & 4.6]
possible data protection risks;	
law enforcement provisions including insolvency law that would apply in case of Cloud Service Provider failure;	[4.6]
Risks to prevent effective supervision, such as execution of audit rights by: (i) (i) statutory auditors (ii) the undertaking (iii) any third party appointed for that purpose (iv) competent authority	[4.3]
E. Concentration risks	**EBA Recom. reference [par. #]**
Risk of operational lock-in (i.e. difficult to find a different cloud service provider)	[4.8]
F. Data and information security risks	**EBA Recom. reference [par. #]**
Risk of losses (e.g. fines, lawsuits, and contractual penalties), reputational damages (e.g. impacts on brand reputation) or impact on perspective revenues due to:	
With reference to the supervised entity, inadequate: (i) data classification and assessment; (ii) identification of data protection measures (e.g. encryption, integrity, traceability); (iii) back-up requirements/management; (iv) IT security and cybersecurity process	[4.5]
With reference to the cloud service providers: (i) poor data and information management (i.e. data confidentiality and information integrity and availability); (ii) IT security incidents (iii) poor service performance (iv) back-up management; (v) IT security and cybersecurity; (vi) other operational risks (e.g. data lock-in).	[4.5]

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU Publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

Westhafenplatz 1,
60327 Frankfurt am Main, Germany

Publications Office