IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

aii 10 years
access to insurance initiative

Cloud Computing: Regulatory and Supervisory Approaches

Report of the A2ii – IAIS Consultation Call

NOV
2019

The Consultation Calls are organised as a partnership between the Access to Insurance Initiative (A2ii) and the International Association of Insurance Supervisors (IAIS) to provide supervisors with a platform to exchange experiences and lessons learnt in expanding access to insurance.

Introduction

The use of cloud computing is becoming more common in the financial sector, including insurance. Alongside the increasing use of new digital technologies, insurers are now able to use cloud services to drive innovation and support critical functions such as underwriting and product development. Cloud computing has benefits but also introduces potential risks, such as those related to data security and confidentiality, as well as the vulnerability of information technology (IT) systems to cyber attacks.[1] It is therefore important for insurance supervisors to consider regulatory requirements and supervisory practices that may be required for cloud computing.

The expert input on this consultation call was prepared by Denise Garcia Ocampo from the Financial Stability Institute (FSI), who also presented on the English and Spanish calls. Andrea Camargo from the A2ii presented the expert input on the French call. Lázaro Cuesta Barberá (European and Occupational Pensions Authority (EIOPA)), Paulo Miller and Gustavo Adolfo Araujo Caldas (Superintendência de Seguros Privados (SUSEP), Brazil) as well as Sanjeev Chandran (Prudential Regulation Authority (PRA) at the Bank of England (BOE), United Kingdom (UK)) joined them to share experiences from their jurisdictions.

The following sections, up until the case studies, are a summary of FSI Insights paper on "Regulating and supervising the clouds: emerging prudential approaches"[2]

Digitalisation of the Insurance Business

Digital technologies are transforming various areas of the insurance value chain. Emerging technologies such as internet of things (IoT) and advanced analytics (AA) are providing real-time information and extensive insights into customer needs, preferences and risk behaviour. These resources help insurers tailor their products and prices to specific customer profiles. Other applications of technologies like machine learning (ML) and artificial intelligence (AI) such as chatbots, robo-advisors or virtual claim adjusters let insurers automate distribution, marketing, underwriting and claims management processes. Distributed ledger technology (DLT) is being used to raise efficiency, reduce costs and lessen the need for intermediation.

Cloud computing is a model that could provide a further boost to the application of digital technologies via an efficient, scalable and flexible arrangement. Insurers can offer products and services based on data collected by IoT, processed by AA, ML, AI or structured via DLT, using

1 The Financial Stability Board (FSB) published a report on "Third-party dependencies in cloud services: Considerations on financial stability implications" available here: https://www.fsb.org/wp-content/uploads/P091219-2.pdf

2 The full paper can be accessed here: https://www.bis.org/fsi/publ/insights13.pdf

available-on-demand shared networks, servers, storage, applications and services that can be rapidly scaled up or down and accessed anytime and anywhere. Cloud computing may help insurers to rapidly respond to customer needs and flexibly adapt to market and technological change.

Cloud Computing: Use in the Insurance Sector

Insurers have made increasing use of cloud computing in recent years.[3] Cloud services were initially applied to business support functions, such as customer management or collaboration applications. Currently, cloud computing is being used in core business functions, such as product development, distribution, underwriting or claims administration. This brings a number of benefits and risks for the insurance sector.

The benefits and risks associated with cloud computing will depend on the particular deployment and service model.[4] In terms of benefits, cloud computing lets insurers share available-on-demand networks, servers, storage, application and services that can be rapidly scaled up or down and accessed anytime and anywhere. In this way, cloud computing allows insurers to quickly launch new products and services, make business processes more efficient and reduce information technology (IT) costs.

Risks that arise from the use of third-party cloud computing services may be different from traditional outsourcing arrangements. This is due to the unique characteristics of cloud computing arrangements, such as:

- Shared computing resources in some cloud deployment models
- The type of information that is stored and processed
- The different geographical location of computing resources and providers
- The small number of global cloud providers, resulting in market concentration that could have systemic implications. The cross-border nature of cloud services complicates the effective oversight of all these risks.

Cloud Computing: Regulatory and Supervisory Approaches

The FSI paper provides an overview of emerging approaches to the regulation and supervision of cloud computing in the insurance industry, drawing upon public information and interviews conducted in 14 financial authorities located in Asia, Europe and North America.

3 See UK case study below.

4 For more details on the different types of cloud computing models, see pages 5-9 of the FSI Insights paper.

Regulatory approaches and requirements

There are currently a range of different regulatory approaches being adopted by the 14[5] insurance supervisory authorities covered in the paper (Table 1). These can be broadly divided into four categories:

- **Applying the relevant regulations of the general outsourcing framework to cloud computing.** Authorities that follow this approach include APRA, OSFI, HKIA, IRDAI, SAMA, MAS, FINMA and FCA. Cloud computing is either assumed to fall under these regulations, or a specific section is allocated to cloud computing within the regulations (e.g. MAS). In general, outsourcing frameworks are based on the Joint Forum high-level principles on outsourcing.[6]
- **Applying the relevant regulations of the governance and risk management framework to cloud computing.** Authorities that follow this approach include the ones that apply the EU Solvency II Directive, where outsourcing provisions are part of the governance and risk management framework (EIOPA, ACPR, BaFin, DNB and PRA) as well as other authorities with governance and risk management regulations, such as APRA, HKIA, IRDAI, FINMA and NAIC.
- **Applying the relevant regulations of the information security framework to cloud computing.** Authorities that follow this approach include APRA, OSFI, BaFin, IRDAI, SAMA, MAS and NAIC. While these regulations are generally relevant to the use of cloud computing, IRDAI, SAMA and MAS include specific sections on cloud-specific requirements. Information security regulations are usually based on the G7's Fundamental Elements of Cybersecurity for the Financial Sector.[7]
- **Cloud-specific recommendations or supervisory expectations.** APRA, OSFI, ACPR, BaFin, DNB and FCA have either provided guidance/recommendations or clarified their regulatory expectations in circulars, memos, sound practices papers and other published materials on the use of cloud computing.
- **Applying the relevant regulations of the information security framework to cloud computing.** Authorities that follow this approach include APRA, OSFI, BaFin, IRDAI, SAMA, MAS and NAIC. While these regulations are generally relevant to the use of

5 Australian Prudential Regulation Authority, Australia (APRA), Office of the Superintendent of Financial Institutions (OSFI) Canada, European Insurance and Occupational Pensions Authority, European Union (EIOPA), Autorité de Contrôle Prudentiel et de Résolution (ACPR) France, Federal Financial Supervisory Authority (BaFin) Germany, Insurance Authority, Hong Kong (HKIA), Insurance Regulatory and Development Authority of India (IRDAI) India, De Nederlandsche Bank (DNB) Netherlands, Saudi Arabian Monetary Authority (SAMA) Saudi Arabia, Monetary Authority of Singapore (MAS) Singapore, Swiss Financial Market Supervisory Authority (FINMA) Switzerland, Financial Conduct Authority (FCA) United Kingdom, Prudential Regulation Authority (PRA) United Kingdom, National Association of Insurance Commissioners (NAIC) United States.

6 The Joint Forum was established under the aegis of the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS) to deal with issues common to the banking, securities and insurance sectors, including the regulation of financial conglomerates. The principles can be accessed here: https://www.bis.org/publ/joint12.htm

7 Available at : https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

cloud computing, IRDAI, SAMA and MAS include specific sections on cloud-specific requirements. Information security regulations are usually based on the G7's Fundamental Elements of Cybersecurity for the Financial Sector.[8]

- **Cloud-specific recommendations or supervisory expectations.** APRA, OSFI, ACPR, BaFin, DNB and FCA have either provided guidance/recommendations or clarified their regulatory expectations in circulars, memos, sound practices papers and other published materials on the use of cloud computing.

Supervisory authority regulations and statement applying to outsourcing to the cloud

Frameworks	Outsourcing		Governance and risk management		Information security	
	General	Cloud specific	General	Cloud specific	General	Cloud specific
APRA	■	■	■		*	■
OSFI	■	■			■	
EIOPA			■			■
ACPR			■	■		
BaFin			■	■	*	■
HKIA	■		■			
IRDAI	■		■		■	■
DNB			■	■		
SAMA	■				■	■
MAS	■	■			■	■
FINMA	■		■			
FCA	■	■				
PRA			■			
NAIC			■		■	

* Currently under consultation process

Note: ■ General framework ■ Cloud-specific statement ■ General framework with a specific section on cloud

Table 1: Regulatory approaches to cloud computing

In terms of areas where requirements are focused, current supervisory material on cloud computing mainly focus on governance, risk assessment, data protection and security, business continuity and exit strategies.[9] The survey conducted across the 14 authorities also revealed that regulatory frameworks have a number of common requirements and expectations for cloud computing. Authorities generally focus on:

8 Available at: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

9 See the FSI Insights paper for the full analysis. The study narrowed down a list of regulatory areas relating to outsourcing, governance and risk management, and information security, and compared between requirements that apply generally and cloud-specific requirements. The paper examines the different regulatory areas such as materiality, governance, due diligence, risk assessment, data protection and security, location, subcontracting, business continuity and exit strategy, monitoring and control and audit and access.

- The adequacy of information security and data confidentiality
- The strength of IT and cybersecurity capabilities of cloud service providers
- The effectiveness of recovery and resumption capabilities
- The adequacy of audit rights, meaning the supervisory authority's access to documentation and information, and the ability to conduct onsite inspections at the provider.

Authorities generally use non-binding guidance through principles and recommendations, adopting a proportionate approach that is tailored to reflect the size, complexity or risk profile of financial institutions or the outsourced service.

Supervision of cloud computing

Authorities have different approaches to supervising the use of cloud computing services by insurers. How insurers are required to communicate their cloud computing plans to the supervisor also varies, ranging from a notification, consultation to authorisation (Table 2).

	Notification	Consultation or authorisation
APRA	Yes, for outsourcing arrangements involving cloud low inherent risks.	Consultation, for outsourcing arrangements involving material activities where offshoring is involved and for arrangements involving cloud heightened or extreme inherent risks regardless of whether offshoring is involved.
OSFI	No	No
EIOPA	Yes, for outsourcing arrangements involving critical or important functions.	No
ACPR	Yes, for outsourcing arrangements involving critical or important functions.	No
BaFin	Yes, for outsourcing arrangements involving critical or important functions.	No
HKIA	Yes, for material outsourcing arrangements.	No
IRDAI	No	No
DNB	Yes, for material outsourcing arrangements.	A form of consultation is required.
SAMA	No	Authorisation, for material outsourcing and for any cloud service arrangement.
MAS	No	No
FINMA	No	Authorisation, for outsourcing arrangements involving significant or control functions relevant to the business plan.
FCA	Yes, for material outsourcing arrangements.	No
PRA	Yes, for outsourcing arrangements involving critical or important functions	No
NAIC	No	No

Table 2: Communication of cloud computing plans

In general, cloud computing is supervised as part of insurers' operational risk reviews, with offsite and onsite reviews and in line with a risk-based approach. Onsite inspections include review of:

- Supporting documentation e.g. prior due diligence and risk assessment of the activity to be outsourced, as well as the outsourcing agreement itself
- The insurer's processes in relation to cyber security management, monitoring of reports and controls, and business continuity plans

Offsite reviews focus on assessing the insurer's governance and risk management practices, and include:

- Notification or approval filing sent to authorities
- Public information e.g. certifications and assurance reports of a cloud service provider
- Regulatory reports on outsourcing activities e.g. an insurer's outsourcing policy, own risk and solvency assessments (ORSA), outsourcing reports
- Thematic reviews and specific questionnaires to obtain specific information on the insurer's cloud computing activities

Other considerations

The paper yielded a number of key findings and considerations for insurance supervisors:

- Although cloud computing is often already subject to general outsourcing requirements, there is value in clarifying cloud-specific regulatory expectations in order to:
  - address the potential specific risks associated with cloud computing
  - provide regulatory certainty with respect to the use of cloud services
  - support market participants in the responsible adoption of the technology
- Any arising regulatory frameworks and requirements would ideally be principles-based, technology-neutral, consistent between financial sectors and applied on a proportionate basis
- International cooperation among home and host authorities, particularly in sharing relevant information on cloud service providers, is especially important to ensure effective oversight of cloud computing activities

The FSI Insights Paper No. 13 "Regulating and supervising the clouds: emerging prudential approaches for insurance companies" (Crisanto, Donaldson, Garcia Ocampo and Prenio, 2018) can be accessed directly here.

CASE STUDY: BRAZIL

The Brazil case study was presented by Paulo Miller and Gustavo Adolfo Araujo Caldas from SUSEP, Brazil

Insurers in the Brazilian market currently use cloud computing services mainly to support non-core activities and functions such as human resources and management activities among others. The market is seeing a growing number of InsurTech companies, which might increase the use of cloud services by insurers. The main cloud service providers in the Brazilian market are Amazon, Microsoft and Google. The main benefits of cloud computing have been increased scalability and with increased digitalisation, dedicated time for companies to focus on other aspects of the business. One of the main challenges facing providers has been migration from one service provider to another.

In terms of regulation, SUSEP is in the initial stages of actively monitoring market behaviour and trends as well as engaging market players in order to determine whether to issue specific regulation regarding the use of cloud computing.

There is currently no specific regulatory framework relating to the use of cloud computing in the insurance sector in Brazil. A recently issued central bank resolution on cybersecurity and cloud services (Res CMN nº 4.658/2018) currently serves as a benchmark and reference for cloud outsourcing services and activities in the insurance market. The regulation requires entities to issue notifications to the central bank, who has veto powers and can place additional requirements. The central bank allows entities to store their data in servers abroad, subject to a requirement in the contract that stipulates that the bank has the right to access the data. Similar to the General Data Protection Regulation (GDPR), confidentiality of personal data is of key importance.

For questions or more information on the relevant activities of SUSEP, please contact gustavo.caldas@susep.gov.br or paulo.vianna@susep.gov.br

CASE STUDY: UK

The UK case study was presented by Sanjeev Chandran from the PRA, Bank of England, UK

In 2019, the PRA conducted a survey that sought to identify and gain a broader perspective on the use of cloud computing services by insurers in the UK. The survey was sent to 30 of the largest insurers and revealed that:

- The use of cloud services among insurers is high (74% of respondents), but still lower than banks
- Most insurers adopt the SaaS service model
- Both critical and sensitive functions are being migrated to the cloud
- The main functions insurers are outsourcing to the Cloud include business management (16%) and customer relationship management (CRM) (16%) (see Figure 1 below)

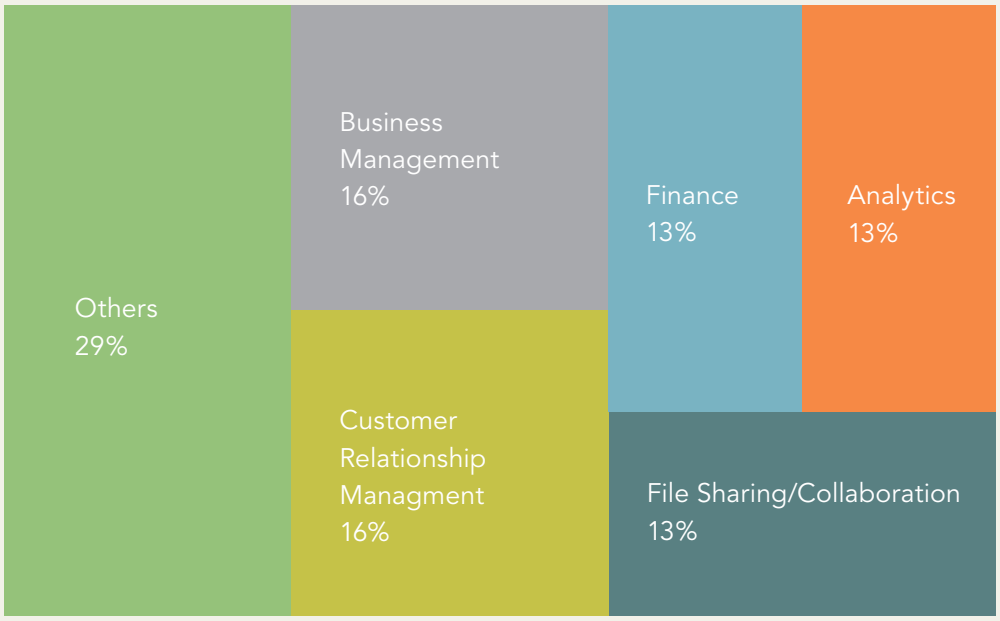

Figure 1: Proportion of applications that use cloud computing services, broken down by function (PRA insurer cloud survey, 2019)

The PRA's regulatory focus with respect to the use of cloud services in the financial sector has been on building operational resilience of financial institutions. In general, insurers in the UK are required to notify the PRA regarding any material outsourcing arrangements. This includes the use of cloud computing. Over time, specific recommendations and guidelines for cloud outsourcing arrangements have been issued for financial services firms in the UK, as summarised in the timeline below (see Figure 2 below):

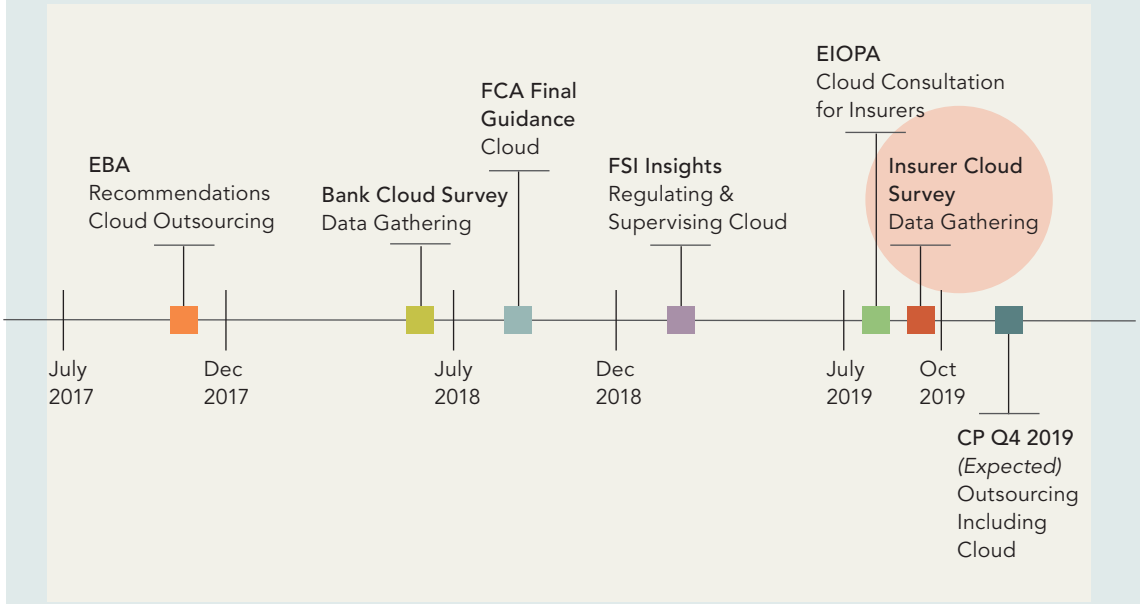

Figure 2: Timeline of establishing recommendations and guidelines for cloud sourcing arrangements in the UK

A key thrust of the PRA's current regulatory approach is to draw on macro-level supervision to inform micro-level supervision. On this, there are three questions that are important to take into consideration when a firm is migrating its functions to the cloud:

- The management and governance of the firm – what is the shared responsibility model of the firm?
- Where the data is being stored and its security – what is the specific location of the cloud service provider and who has the right to audit the data?
- Risk of concentration of cloud service providers and ease of substitutability – Can the firm easily change its outsourcing arrangement(s)? What negotiating powers does the insurer have?

Looking ahead, the PRA will continue to develop their approach to micro-level supervision in three ways: align supervisory approaches between the banking and insurance sectors, ensure that all international guidelines are met where relevant, and, consistent with risk-based supervision, focus on where there is likely to be maximum impact.

Key insights gained so far include the following:

- It is important to view cloud computing in the broader context of operational resilience.
- There is a need to establish a "base-level" against which firm's cloud strategies can be assessed. Supervisors are currently in the early days of their experience with cloud.
- It is important for insurance supervisors to understand the micro- and macro-level linkages. This means learning from individual firm reviews as well as sector-wide initiatives.

- Extra-sectoral factors need to be considered as well. Beyond aligning with banking, it may be important to also consider how non-financial industries are using cloud.
- There is a need to ensure consistency in regulatory approaches across different jurisdictions.

For questions or more information on the relevant activities of the PRA, please contact Sanjeev.Chandran@bankofengland.co.uk

CASE STUDY: EIOPA

The Taiwan case study was presented by Thomas Chang from the Financial Supervisory Commission of Taiwan (FSC).

This case study draws on the EIOPA report "Outsourcing to the Cloud: EIOPA's Contribution to the European Commission Fintech Action Plan" (2019)[10] and EIOPA "Consultation paper on the proposal for Guidelines on outsourcing to cloud service providers" (2019).[11] The results of a survey on the use of cloud computing services revealed that cloud computing is most extensively used by newcomers, within a few market niches and by larger insurers. As part of their wider digital transformation strategies, many European large (re)insurers are expanding their use of the cloud. The level of use is also not homogenous among EU countries.

Under the Solvency II framework, the use of cloud computing by insurers[12] falls within the broader scope of outsourcing[13] under Articles 38 and 49 of the Solvency II Directive and Article 274 of the Solvency II Delegated Regulation. The EIOPA Guidelines on System of Governance also provide principles-based guidance. The applicable regulations focus mainly on governance and risk management. A key general provision is that the responsibility for outsourced activities and functions must stay within the insurer, and insurers should have a written outsourcing policy. The Solvency II Directive (Article 49 (2)) has also placed certain limits on outsourcing of critical or important operational functions and activities. Among others, such activities should not be undertaken in a way that leads to any of the following:

- Materially impairing the quality of the system of governance of the insurer
- Unduly increasing the operational risk
- Impairing the ability of the supervisory authorities to monitor the compliance of the insurer with its obligations
- Undermining continuous and satisfactory service to policyholders

In terms of supervisory requirements, insurance entities are required to notify the supervisor regarding any material activities and developments, prior to outsourcing those activities/functions and all subsequent ones. In addition, insurance entities are required to have a written outsourcing agreement and inform the supervisors of its content, as well as the criteria applied in choosing the cloud services provider.

10 Available at: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_outsourcing_to_the_cloud_contribution_to_fintech_action_plan_3_0.pdf

11 Available at https://www.eiopa.europa.eu/content/consultation-proposal-guidelines-outsourcing-cloud-service-providers_en

12 All references to 'insurers' in this section includes reinsurers.

13 Article 13(28) of the Solvency II Directive states that: 'outsourcing' means an arrangement of any form between a (re)insurance 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 (re)insurance undertaking itself.

However, some regulatory areas that are unique to cloud computing still need to be clarified. These include the following:

- Application of the regulatory definition of outsourcing to the purchase of cloud services
- Risk and materiality assessment and notification to competent authorities prior to entering into cloud outsourcing arrangements
- Management of specific risks associated with the use of cloud computing services (e.g. data and systems security, confidentiality, legal and reputational risk, concentration risk)
- Application of the audit and access requirements to cloud arrangements
- Supervision of cloud outsourcing arrangements

From July-September 2019, EIOPA launched a public consultation on the proposal for guidelines on outsourcing to cloud service providers.[14] Of relevance in this context, is the guideline on "Supervision of cloud outsourcing arrangements by supervisory authorities" which stipulates that within their assessments, supervisory authorities should assess the following aspects using a risk-based approach:

- Governance of outsourcing arrangements
- Availability of sufficient resources, adequate skills and knowledge to monitor cloud outsourcing activities
- Risks (e.g. operational, reputational, IT risks, strategic and concentration risks) associated with cloud outsourcing

There are special provisions regarding on-site inspections carried out at cloud service providers' premises. Supervisory authorities are required to have the knowledge and experience to supervise these requirements e.g. IT and cybersecurity knowledge, business continuity management etc. Supervisory authorities can take the following possible actions where concerns are identified: improving the governance arrangement, limiting or restricting the scope of the outsourced functions or requiring exit from one or more outsourcing arrangements.

The draft guidelines took into consideration the EIOPA's Contribution to the European Commission Fintech Action Plan (March 2019) and the European Banking Authority (EBA) recommendations on outsourcing to cloud service providers. The guidelines are due to be adopted in 2020.

For questions or more information on the relevant activities of EIOPA,
please contact Lazaro.Cuesta@eiopa.europa.eu

14 Available at: https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers

Questions and Discussion

How can supervisors carry out on-site reviews/inspections when the cloud server is located in another jurisdiction, especially in countries without a cooperation agreement? This is one often-debated topic for supervisors. Onsite inspection would be very challenging for supervisors as it requires a lot of expertise and resources. The most important thing is for supervisors to have auditing rights to the cloud provider facilities. In practice, as far as experts on the call are aware, there has not been a case where supervisors actually exercised this right. There was only one particular case where onsite review took place: in one jurisdiction, one cloud service provider served 70% of the market. There were also very specific technical issues on security which supervisors needed to understand. In all other cases however, supervisors have held meetings locally in their jurisdiction with the cloud service provider to understand the agreements and conditions within the outsourcing agreement. Each agreement is always different, and it is important to understand unique features of the contracts. In general, the use of cloud is in early stages and best practices will become more evident over time.

At the 2019 IAIS Annual Conference, one prominent cloud service provider expressed that they would like to be more included in supervisory discussions with regard to regulating cloud. What is your view on this? It is important that supervisors maintain contact and constant dialogue with cloud service providers. Supervisors need to understand how cloud service providers function, the features of the services provided and the security implications on the insurer. Cloud service providers also need to understand supervisors, the risks supervisors see from their perspective and the respective regulatory requirements. As such it would useful for supervisors and cloud service providers to have a direct communication line and develop a mutual understanding.

If cloud computing is an outsourcing arrangement, why should there be a special notification requirement to the supervisor, instead of being treated like any other outsourcing function? Under the Solvency II directive at least, insurers are required to notify the supervisory authority in all cases where critical functions are outsourced, and this applies equally to cloud outsourcing. The customisation is in the content and information required in the notification, where supervisors might request specific information that is unique to the characteristics of cloud computing. Such unique information that may be useful to clarify to supervisors includes, for example, the use, types and storage of data impacted by the cloud arrangement.

What are best practices or lessons so far, such as "do's and don'ts"? The use of cloud for critical functions is still early stages, but some initial advice would be for supervisors to have robust regulatory reports on cloud computing arrangements in order to obtain detailed information that they can use to assess whether insurers are adequately managing the risks related to the use of the cloud. Supervisors should not rush to regulate before assessing the status of cloud computing services in their markets. It is important for supervisors to assess if and how cloud computing is being used in their market in order to identify ways to regulate it. SUSEP shared their approach so far is to largely align with the banking sector, which at this point is focused on guaranteeing in the contract that supervisors should have access to the data and confidentiality of personal data.

Implementation Partner:

IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Supported by:

Federal Ministry for Economic Cooperation and Development

Ministry of Foreign Affairs of the Netherlands

Hosted by:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Access to Insurance Initiative
Hosted by GIZ Sector Project
Financial Systems Approaches to Insurance
Deutsche Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Telephone: +49 61 96 79-1362
Fax: +49 61 96 79-80 1362
E-mail: secretariat@a2ii.org
Internet: www.a2ii.org

a2ii_org

Promoting access to responsible, inclusive insurance for all.