EIOPA-BoS-19/270
1 July 2019

Consultation paper on the proposal for Guidelines on outsourcing to cloud service providers

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany - Tel. + 49 69-951119-20;
Fax. + 49 69-951119-19; email: info@eiopa.europa.eu site: https://eiopa.europa.eu/

1 Table of Contents

Responding to this paper

1. EIOPA welcomes comments on the proposal for Guidelines on outsourcing to cloud service providers.

2. Comments are most helpful if they:

a. respond to the question stated, where applicable;

b. contain a clear rationale; and

c. describe any alternatives EIOPA should consider.

3. Please send your comments to EIOPA by 30 September 2019 responding to the questions in the survey provided at the following link:

   https://ec.europa.eu/eusurvey/runner/Consultation_Cloud_GL_2019

   Contributions not provided using the survey or submitted after the deadline will not be processed and therefore considered as if they were not submitted.

Publication of responses

4. Contributions received will be published on EIOPA's public website unless you request otherwise in the respective field in the template for comments. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure.

5. Please note that EIOPA is subject to Regulation (EC) No 1049/2001 regarding public access to documents and EIOPA's rules on public access to documents[1].

6. Contributions will be made available at the end of the public consultation period.

Data protection

7. Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published. They will only be used to request clarifications if necessary on the information supplied. EIOPA, as a European Authority, will process any personal data in line with Regulation (EC) No 45/2001 on the protection of the individuals with regards to the processing of personal data by the Community institutions and bodies and on the free movement of such data. More information on data protection can be found at https://eiopa.europa.eu/ under the heading 'Legal notice'.

Consultation paper overview & next steps

8. EIOPA carries out consultations in the case of Guidelines and Recommendations in accordance with Article 16(2) of Regulation (EU) No 1094/2010. This Consultation Paper presents the draft Guidelines.

9. The analysis of the expected impact from the proposed policy is covered under Annex I (Impact Assessment).

Next steps

10. EIOPA will consider the feedback received and expects to publish a Final Report on the consultation and to submit the Guidelines for adoption by its Board of Supervisors.

[1] Public Access to Documents

Background

11. Under Article 16 of Regulation (EU) No 1094/2010 EIOPA may issue Guidelines and Recommendations addressed to competent authorities and financial institutions with a view to establish consistent, efficient and effective supervisory practices and ensuring the common, uniform and consistent application of Union law.

12. In accordance with Article 16(3) of that Regulation, competent authorities and financial institutions are required to make every effort to comply with those Guidelines and Recommendations.

13. EIOPA identified the need to develop specific guidance on outsourcing to cloud service providers in the context of the analysis performed to answer the European Commission FinTech Action plan (COM(2018) 109 final) and following discussions and exchanges with stakeholders[2].

14. Cloud services are a combination of a business and delivery model that enable on-demand access to a shared pool of resources such as applications, servers, storage and network security. The service is typically delivered in the form of Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

15. Compared with more traditional forms of outsourcing offering dedicated solutions to clients, cloud outsourcing services are much more standardised, which allows the services to be provided to a larger number of different customers in a much more automated manner and on a larger scale. Although cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness, they also raise challenges in terms of data protection and location, security issues and concentration risk, not only from the point of view of individual undertakings but also at industry level, as large suppliers of cloud services can become a single point of failure when many undertakings rely on them.

16. EIOPA acknowledges that, compared to traditional IT systems, in cloud based systems, the cloud service provider and cloud customer share the control of a cloud system's resources. The cloud's different service models affect their (i.e. cloud provider and cloud customer) control over the computational resources and, thus, what can be done in cloud based systems. This means that, also from a security and control perspective, the cloud provider and the cloud customer might share responsibilities. Nonetheless, insurance and reinsurance undertakings remain responsible for complying with all their regulatory obligations when they outsource, including to cloud service providers.

17. The use of cloud outsourcing is a practice common to all financial undertakings[3] and not only to insurance and reinsurance undertakings. Moreover, the main risks associated to this practice are similar across sectors. Acknowledging this, and recognising the potential risks of regulatory fragmentation in this area, EIOPA has considered the most recent guidance published by the European Banking Authority (EBA) on this field: the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) and the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), which have been integrated into the EBA Guidelines on outsourcing and are repealed with effect from 30 September 2019.

[2] The report published by EIOPA as answer to the European Commission FinTech Action plan can be obtained here

[3] As defined by Article 13 (25) of Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), (OJ L 335, 17.12.2019, p. 1)

18. The aims of these Guidelines are to:

a. provide clarification and transparency to market participants avoiding potential regulatory arbitrages;

b. foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing.

Guidelines on outsourcing to cloud service providers

Introduction

1. In accordance with Article 16 of Regulation (EU) No 1094/2010[4] EIOPA is issuing these Guidelines to provide guidance to insurance and reinsurance undertakings on how the outsourcing provisions set forth in Directive 2009/138/EC[5] ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/35[6] ("Delegated Regulation") needs to be applied in case of outsourcing to cloud service providers. To that end, these Guidelines build on Articles 13(28), 38 and 49 of the Solvency II Directive and Article 274 of the Delegated Regulation. Moreover, these Guidelines build also on the guidance provided by EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253).

2. These Guidelines are addressed to competent authorities and to insurance and reinsurance undertakings (collectively 'undertaking(s)').

   The Guidelines apply to both individual undertakings and *mutatis mutandis* for groups[7]. When the Guidelines refer to entities that are part of the group, in general, they refer to insurance and reinsurance undertakings.

3. Undertakings and competent authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality[8], and the materiality of the service outsourced to cloud service providers. The proportionality principle aims at ensuring that governance arrangements, including those related to outsourcing to cloud service providers, are consistent with the nature, scale and complexity of their risks.

4. These Guidelines should be read in conjunction with and without prejudice to EIOPA Guidelines on system of governance and to the regulatory obligations listed at paragraph 1.

5. If not defined in these Guidelines, the terms have the meaning defined in the legal acts referred to in the introduction.

6. In addition, for the purposes of these Guidelines, the following definitions apply:

Function	means any processes, services or activities.
Material outsourcing	means the outsourcing of critical or important operational functions or activities as further specified by Guideline 7.
Outsourcing process	means all the activities performed by the undertakings to plan, contract, implement, monitor, manage and terminate outsourcing arrangements.

[4] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pension Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[5] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), (OJ L 335, 17.12.2019, p. 1).

[6] Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), (OJ L 12, 17.1.2015, p. 1).

[7] As defined by Article 212 (1) of Directive 2009/138/EC.

[8] The application of the principle of proportionality, in the context of these Guidelines, should be done in accordance with Article 29 of Directive 2009/138/EC.

Service provider	means a third party entity that is performing an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.
Cloud service provider	means a service provider responsible for delivering cloud services under an outsourcing arrangement. Arrangements with third parties which are not cloud service providers but rely significantly on cloud infrastructure to deliver their services (for example, where the cloud service provider is part of a sub-outsourcing chain) fall within the scope of these Guidelines. The same principle is applied to the cloud brokers.
Cloud broker	means 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 service provider directly.
Significant sub-outsourcer	means service provider responsible for delivering cloud services to the main provider with whom the undertaking has a contractual agreement in place; a sub-outsourcer is significant when the main agreement would not work without an effective and safe delivery of sub-outsourced services.
Cloud services	means 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[9].
Public cloud	means cloud infrastructure available for open use by the general public.
Private cloud	means cloud infrastructure available for the exclusive use by a single undertaking.
Community cloud	means cloud infrastructure available for the exclusive use by a specific community of undertakings, e.g. several undertakings of a single group.
Hybrid cloud	means cloud infrastructure that is composed of two or more distinct cloud infrastructures.

7. These Guidelines apply from 01 July 2020 to all cloud outsourcing arrangements entered into or amended on or after this date.

8. Undertakings should review and amend accordingly existing cloud outsourcing arrangements with a view to ensuring that these are compliant with these Guidelines by 01 July 2022.

[9] The cloud services are typically delivered to the undertakings in the form of Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

9. Where the review of material cloud outsourcing arrangements is not finalised by 01 July 2022, an undertaking should inform its supervisory authority[10] of that fact, including the measures planned to complete the review or the possible exit strategy. Then, the supervisory authority may agree with the undertaking on an extended timeline for completing that review where appropriate.

Questions to stakeholders

Q1. Is the scope of application provided appropriate and sufficiently clear?

Q2. Is the set of definitions provided appropriate and sufficiently clear?

Q3. Is the timeline to implement the Guidelines considered sufficient to ensure a smooth transition from the current operational practices to the ones provided by these Guidelines?

Guideline 1 – Cloud services and outsourcing

10. The undertaking should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing (Article 13(28) of the Solvency II Directive). As a rule, outsourcing should be assumed. Within the assessment, consideration should be given to:

a. whether the function (or a part thereof) outsourced is performed on a recurrent or an ongoing basis; and

b. whether this function (or part thereof) would normally fall within the scope of functions that would or could normally be performed by the undertaking in the course of its regular business activities, even if the undertaking has not performed this function in the past.

11. Where an arrangement with a service provider covers multiple functions, the undertaking should consider all aspects of the arrangement within its assessment.

12. As part of their internal control system, taking into account the principle of proportionality and the materiality of the function outsourced, the undertaking should identify, measure, monitor, manage and report risks caused by arrangements with third parties regardless whether or not those third parties are cloud service providers.

Questions to stakeholders

Q4. Is the Guideline on cloud services and outsourcing appropriate and sufficiently clear to enable the distinction between cloud services falling within the scope of outsourcing and the ones not falling within such scope?

Guideline 2 - General principles of governance for cloud outsourcing

13. The decision to enter into a material outsourcing[11] with cloud service providers should be taken by the undertaking's administrative, management or supervisory body (AMSB). That decision should be based on a thorough risk assessment including all relevant risks implied by the arrangement such as IT and operational risks, business continuity risk, legal and compliance risks, concentration risk and, where applicable, risks associated to the data migration and/or the IT implementation phase.

[10] As defined by Article 13 (10) of Directive 2009/138/EC.

[11] An undertaking establishes the materiality of its cloud outsourcing arrangements according to the provisions described in Guideline 7.

14. The undertaking, where appropriate, should reflect the changes on its risk profile due to its cloud outsourcing arrangements within its own risk and solvency assessment ('ORSA').

15. The use of cloud services should be consistent with the undertaking's strategies (e.g. IT strategy) and internal policies and processes which should be updated, if needed.

Guideline 3 – Written policy on outsourcing to cloud service providers

16. In case of outsourcing to cloud service providers, the undertaking should update the written outsourcing policy, taking into account cloud computing specificities at least in the following areas:

a. the roles and responsibilities of the functions involved in case of outsourcing to cloud service providers (in particular: AMSB, IT function, compliance function, risk management function and internal audit);

b. the processes and reporting procedures required for the approval, implementation, monitoring, management and renewal, where applicable, of cloud outsourcing arrangements;

c. the oversight of the cloud services including (i) risk assessments and due diligence on cloud service providers, including their frequency; (ii) monitoring and management controls (e.g. verification of the service level agreement); (iii) security standards and controls;

d. contractual requirements for material and non-material cloud outsourcing arrangements;

e. documentation requirements and written notification to the supervisory authority; and

f. documented strategies to exit ('exit strategies') material outsourcing and to terminate ('termination processes') the cloud outsourcing arrangements regardless of their materiality.

Questions to stakeholders

Q5. Is the Guideline on written policy appropriate and sufficiently clear to manage the undertaking's roles, processes and procedures on outsourcing to cloud service providers? Is it consistent with the market best practices on defining the policy for general outsourcing?

Guideline 4 - Written notification to the supervisory authority

17. The written notification requirement set in Article 49(3) of the Solvency II Directive and further detailed by EIOPA Guidelines on System of Governance (Guideline 64) are applicable to all material cloud outsourcing identified according to Guideline 7.

18. The undertaking's written notification to the supervisory authority for material cloud outsourcing should include, in addition to a draft version of the outsourcing agreement, and taking into account the principle of proportionality, at least the following information:

a. the function outsourced and its interconnections with other critical or important functions;

b. the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the undertaking;

c. the governing law of the cloud outsourcing agreement;

d. in case of groups, the insurance or reinsurance undertakings and other undertakings within the scope of the prudential consolidation, where applicable, that make use of the cloud services;

e. the name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any); in case of groups, whether or not the cloud service provider is part of the group;

f. a description of the activities performed by the cloud service provider, the cloud service models (for example IaaS/PaaS/SaaS), the cloud infrastructure (i.e. public/private/hybrid/community), the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored and processed, the results of the materiality assessment and the date of the more recent materiality assessment;

g. the outcome of the assessment of the cloud service provider's substitutability (e.g. easy, difficult or impossible);

h. whether the undertaking has an exit strategy in case of termination by either party or disruption of services by the cloud service provider, in line with EIOPA Guidelines on System of Governance (Guideline 63);

Questions to stakeholders

Q6. Is the list of information to be notified to the national supervisory authorities considered appropriate to understand the most significant areas taken into account by the undertakings in their decision making process?

Guideline 5 – Documentation requirements

19. As part of their governance and risk management systems, the undertaking should maintain an updated register on all its material and non-material functions outsourced to cloud service providers. Taking into account national regulation and the principle of proportionality, the undertaking should maintain the documentation of past outsourcing arrangements within the register and the supporting documentation for an appropriate retention period.

20. The undertaking should make available to the supervisory authority, on request, the register, a copy of the outsourcing agreement, and related information on the periodical assessment performed, or any parts thereof.

21. Where the register of all existing cloud outsourcing arrangements is established and maintained centrally within a group, supervisory authorities and all undertakings belonging to the group should be able to obtain the section of the register related to an individual undertaking without undue delay.

22. In case of non-material outsourcing, the register should include, where applicable, the information to be notified to the supervisory authority for material cloud outsourcing arrangements referred to in Guideline 4.

23. In case of material outsourcing, the register should include at least the following information:

a. the information to be notified to the supervisory authority for material cloud outsourcing arrangements referred to at Guideline 4;

b. the date of the latest risk assessment and a brief summary of the main results;

c. the decision-making body (e.g. the management body) in the undertaking that approved the cloud outsourcing;

d. the estimated annual costs;

e. the dates of the most recent and next scheduled audits, where applicable;

f. the names of significant sub-outsourcers, if any, including the countries where the sub-outsourcers are registered, where the service will be performed and, if applicable, the locations (i.e. countries or regions) where the data will be stored and processed;

g. whether the cloud service provider (or any significant sub-outsourcer(s)) supports business operations that are time critical;

h. whether the cloud service provider (or any significant sub-outsourcer(s)) has a business continuity plan that is suitable for the services provided to the undertaking in line with Article 274(5)(d) of the Delegated Regulation; and

i. a description of the undertaking monitoring of the cloud outsourced activities (i.e. number of resources and their skills).

Questions to stakeholders

Q7. Would the introduction of a register of all cloud outsourcing arrangement have a significant impact on the current undertakings practices to manage cloud-outsourcing arrangements? What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?

Q8. Are the documentation requirements appropriate and sufficiently clear?

Guideline 6 – Pre-outsourcing analysis

24. Before entering into any arrangement with cloud service providers, the undertaking should:

a. assess if the cloud outsourcing arrangement is material;

b. identify and assess all relevant risks of the cloud outsourcing arrangement;

c. undertake appropriate due diligence on the prospective cloud service provider; and

d. Identify and assess conflicts of interest that the outsourcing may cause in line with the requirements set out in Article 274(3) (b).of the Delegated Regulation.

Guideline 7 – Materiality assessment

25. Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing has to be considered 'material'. The assessment should take into account whether the cloud outsourcing is related to critical or important operational functions as referred to in the Solvency II Directive and in the Delegated Regulation and whether the cloud outsourcing is materially affecting the risk profile of the undertaking. In performing such assessment, where relevant, an undertaking should take into account the possible extension and foreseen changes to the cloud services' scope.

26. The undertaking should consider always as material all the outsourcing of critical or important operational functions to cloud service providers. The identification of

critical or important operational functions should be performed according to EIOPA Guidelines on System of Governance (Guideline 60)[12].

27. Moreover, in order to determine the materiality of cloud outsourcing, undertakings should take into account, together with the outcome of the risk assessment, at least the following factors:

a. the potential impact of outages, disruptive events or failure of the cloud service provider to provide the services at the agreed service levels on the undertaking:
    i. continuous compliance with the conditions of their authorization, and other obligations under the Solvency II Directive;
    ii. short and long-term financial and solvency resilience and viability;
    iii. business continuity and operational resilience;
    iv. operational risk, including conduct, information and communication technology (ICT), cyber and legal risks;
    v. reputational and strategic risks;
    vi. recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation, where applicable.

b. the potential impact of the cloud outsourcing arrangement on the ability of the undertaking to:
    i. identify, monitor and manage all risks;
    ii. comply with all legal and regulatory requirements;
    iii. conduct appropriate audits regarding the function affected by the cloud outsourcing arrangement, in line with Article 38 of the Solvency II Directive;

c. the undertaking's aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same undertaking's business area;

d. the size and complexity of any undertaking's business areas affected by the cloud outsourcing arrangement;

e. the cost of the cloud outsourcing as a proportion of total operating and ICT costs of the undertaking;

f. the potential business interconnections between the undertakings and the cloud service provider. For instance, if the undertaking is providing (re)insurance coverage to the cloud provider;

g. the ability, if necessary or desirable, to transfer the proposed cloud outsourcing arrangement to another cloud service provider or reintegrate the services ('substitutability'); and

h. the protection of personal and non-personal data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the undertaking, policyholders or other relevant subjects including but not limited

[12] "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."

to compliance with Regulation (EU) 2016/679[13]. The undertaking should particularly take into consideration data that is business sensitive and/or critical (e.g. policyholders' health data).

Questions to stakeholders

Q9. Taking into account the specific nature of cloud services, it has been opted to use the concept of 'materiality' to clarify, in this context, the concept of a 'critical or important operational function'. Is this approach appropriate and sufficiently clear?

Guideline 8 – Risk assessment of cloud outsourcing

28. The undertaking should assess the potential impact of material cloud outsourcing both before and after the outsourcing particularly on their operational risk, strategic risk, concentration risk and reputational risk. The assessment should include, where appropriate, scenario analysis of possible but plausible, including high-severity, operational risk events.

29. Moreover, within their risk assessment in case of material cloud outsourcing, the undertaking should also take into account the expected benefits and costs of the proposed cloud outsourcing arrangement performing a cost-benefit analysis to be approved, as part of the overall approval, by the AMSB. The cost-benefit analysis should consider and weigh any significant risks which may be reduced or better managed against any significant risks which may arise as a result of the proposed cloud outsourcing arrangement.

30. Carrying out the risk assessment, the undertaking should, at a minimum:

a. consider the design of the cloud service used;

b. identify and classify the relevant functions and related data and systems as to their sensitivity and required security measures;

c. assess the risks arising from the selected cloud service (i.e. IaaS/PaaS/SaaS) and deployment models (i.e. public/private/hybrid/community);

d. where applicable, assess the risks arising from the migration and/or the implementation;

e. conduct a thorough risk-based analysis of the functions and related data and systems which are under consideration to be outsourced or have been outsourced and address the potential risk impacts, in particular the operational risks, including legal, IT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are or may be provided and where the data are or are likely to be stored or processed;

f. consider the consequences of where the cloud service provider is located, the data are stored or processed (within or outside the EU) including the context of assuring compliance of the provided services with applicable EU and national laws, external and internal regulations and standards adopted by the undertaking;

g. consider the political stability and security situation of the jurisdictions in question, including:

    i. the laws in force, including laws on data protection;

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1).

ii. the law enforcement provisions in place; and

iii. the insolvency law provisions that would apply in the event of a service provider's failure and any constrains that would arise in the respect of the urgent recovery of the undertaking's data in particular;

h. assess the risk of significant sub-outsourcing by the cloud service provider, taking into account:

i. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-outsourcer is located in a third country or a different country from the service provider;

ii. the risk that long and complex chains of sub-outsourcing reduce the ability of the undertaking to oversee its material function and the ability of supervisory authorities to effectively supervise them;

The risk management system applied by the undertaking should take into account the risks related to sub-outsourcing. If the risk is considered too high, the undertaking should not accept sub-outsourcing to a specific sub-outsourcer or third party.

i. assess the concentration risk, including from:

i. outsourcing to a dominant cloud service provider that is not easily substitutable; and

ii. multiple outsourcing arrangements with the same cloud service provider or closely connected service providers;

31. The risk assessment should be performed before entering into a material cloud outsourcing and on a periodical basis, as defined in the written policy, and, in any case, before renewal of the agreement (if it concerns content and scope). Moreover, if the undertaking becomes aware of significant deficiencies and significant changes of the services provided or the situation of the cloud service provider, the risk assessment should be promptly reviewed or re-performed.

Questions to stakeholders

Q10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?

Guideline 9 – Due diligence on cloud service provider

32. Undertakings should perform a due diligence on the cloud service provider applying criteria defined by their written outsourcing policy.

33. The due diligence should include an evaluation of the suitability of the cloud provider (skills, infrastructure, economic situation, corporate and regulatory status, etc.). Where appropriate, evidence / certificates based on common standards (including but not necessarily limited to: International Safety Standard ISO / IEC 2700X of the International Organization for Standardization, C 5 Requirement Catalogue of the Federal Office for Information Security), test reports of recognized third parties or internal test reports of the cloud provider can be used to support the due diligence performed.

Guideline 10 – Contractual requirements

34. The respective rights and obligations of the undertaking and of the cloud service provider should be clearly allocated and set out in a written agreement.

35. In addition to the set of requirements defined by Article 274 of the Delegated Regulation, the written agreement between an undertaking and a cloud service provider for arrangements classified as material should set out at least:

a. a clear description of the cloud services, including the type of support services;

b. the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the undertaking;

c. the court jurisdiction and the governing law of the agreement;

d. the parties' financial obligations including the cloud services pricing model;

e. the parties' operational obligations and responsibilities (for example, in case of updates or in case of user and access management or incident management);

f. whether significant sub-outsourcing is permitted, and, if so, the conditions to which the sub-outsourcing is subject to (see Guideline 13);

g. the location(s) (i.e. regions or countries) where relevant data will be kept and processed, including the possible storing locations (i.e. location of data centres), and the conditions to be met, including a requirement to notify the undertaking if service provider proposes to change the location(s);

h. provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, taking into account the specifications of Guideline 12;

i. the right for the undertaking to monitor the cloud service provider's performance on an on-going basis taking into account the Guideline 14;

j. the agreed service levels which should include quantitative and qualitative performance targets, that are directly measurable by the undertaking in order to independently monitor the services received and, eventually, adopt corrective action if agreed service levels are not met;

k. the reporting obligations of the cloud service provider to the undertaking, including the obligations to submit the reports relevant for the undertaking's internal audit function ;

l. whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

m. the requirements to implement and test business contingency plans;

n. provisions to ensure that the data owned by the undertaking can be promptly recovered by the undertaking in case of the insolvency, resolution or discontinuation of business operations of the cloud service provider.

36. Regarding an outsourcing agreement for material cloud outsourcing, special care should be taken of Article 274(4)(h) to (I) of the Delegated Regulation related to the supervision of outsourced functions and activities ('audit and access rights') and termination and exit rights according to Article 274(4)(d) to (e) of the Delegated Regulation.

37. Moreover, regardless the materiality of the outsourcing, the outsourcing agreement should include all the requirements set out in Article 38 of the Solvency II Directive. In particular, the undertaking should ensure that the outsourcing agreement or any other contractual arrangement do not impede or limit its supervisory authority to carry out its supervisory function and objectives and the effective supervision of outsourced functions and activities.

38. In case of non-material outsourcing, the clauses within the agreement between the undertaking and a cloud service providers should be written taking into account the type of data stored, managed or processed by the cloud service provider (or, where applicable, its significant sub-outsourcers).

Question to stakeholders

Q11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?

Q12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?

Guideline 11 – Access and audit rights

39. The outsourcing agreement should not limit the undertaking's information, access and audit rights as well as control options on cloud services in order to fulfil all its regulatory obligations. Additionally, it should be ensured that the undertaking receives the information it needs to adequately manage and monitor the risks associated with cloud outsourcing arrangements.

40. The undertaking should exercise its access and audit rights, determine the audit frequency and the areas and services to be audited on a risk-based approach, according to Section 8 of EIOPA Guidelines on System of Governance.

41. The scope of the audits should include an assessment of the service provider's and, where applicable, its significant sub-outsourcers' security and control environment, incident management process (in particular in case of data breaches, service disruptions or other material issues) and the undertaking's observance of these Guidelines in relation to cloud outsourcing arrangements.

42. In determining the frequency of audit assessment, the undertaking should consider the nature and extent of risk and impact on the undertaking from the cloud outsourcing arrangements.

43. If the performance of audits or the use of certain audit techniques might create a risk for the environment of the cloud service provider and/or another cloud service provider's client (e.g. impact on service levels, availability of data, confidentiality aspects), the undertaking and the cloud service provider should agree on alternative ways to provide a similar level of assurance to the undertaking.

44. Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organizational burden on the cloud service provider and its customers, undertakings may use:

a. third party certifications and third-party or internal audit reports made available by the cloud service provider;

b. Pooled audits (i.e. performed jointly with other clients of the same cloud service provider), audit performed by third clients or by a third party appointed by them.

45. Undertakings should make use of the method referred to in paragraph 44(a) only if they:

a. are satisfied with the audit plan for the service outsourced to cloud service providers;

b. ensure that the scope of the certification or the audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and the key

controls identified by the undertaking and the compliance with relevant regulatory requirements;

c. thoroughly assess the content of new certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

d. ensure that key systems and controls are covered in future versions of the certification or audit report;

e. are 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);

f. are satisfied that certifications are issued and the audits are performed according to appropriate standards and include a test of the operational effectiveness of the key controls in place;

g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; and

h. retain the contractual right to perform individual on-site audits at their discretion with regard to material outsourcing; such right should be exercised in case of specific needs not manageable through other types of interactions with the cloud service provider.

46. For material cloud outsourcing, the undertaking should assess whether third-party certifications and reports as referred to in paragraph 44(a) are adequate and sufficient to comply with their regulatory obligations but should not rely solely on these reports over time.

47. Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third party acting on behalf of undertaking(s)) should provide prior notice in a reasonable time period of the on-site visit to a relevant business premise, unless an early prior notification has not been possible due to an emergency or crisis situation.

48. Considering that cloud solutions have a high level of technical complexity, the undertaking 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 – or, as appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the appropriate skills and knowledge to perform effective and relevant audits and/or assessments.

Question to stakeholders

Q13. Are the guideline on access and audit rights appropriate and sufficiently clear?

Guideline 12 – Security of data and systems

49. The undertaking should ensure that cloud service providers comply with appropriate IT security and data protection standards. The undertaking should, additionally, define data and system security requirements in the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.

50. For the purposes of the previous paragraph, an undertaking, prior to outsource to cloud service providers, on the basis of the results of the risk assessment performed in accordance with Guideline 8, should:

a. define and decide on an appropriate level of protection of confidential data, continuity of activities outsourced, integrity and traceability of data and systems in the context of the intended cloud outsourcing;

b. ensure 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, and a sound user and access management process;

c. ensure that network traffic availability and expected capacity are guaranteed, where applicable and feasible;

d. define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain including significant sub-outsourcing, where applicable;

e. define specific processes by the undertaking and the cloud service provider to ensure an overall sound management of the incidents that may occur;

f. agree on a data residency policy with the cloud service provider which sets out the countries where the undertaking's data can be stored, processed and managed. This policy should be reviewed periodically and the undertaking should be able to verify compliance of the cloud service provider with such policy; and

g. monitor the level of fulfilment of the requirements relating to the efficiency of control mechanisms implemented by the cloud service provider and its significant sub-outsourcers that would mitigate the risks related to the provided services.

Question to stakeholders

Q14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?

Guideline 13 – Sub-outsourcing

51. To comply with the requirements of Article 274(4)(k) and (l) of the Delegated Regulation, the cloud outsourcing agreement should specify, where relevant, whether or not sub-outsourcing of critical or important functions or activities of the undertaking, or significant parts thereof, are permitted or expressly excluded.

52. The undertaking should agree to sub-outsource only if the sub-outsourcer will also fully comply with the obligations existing between the undertaking and the cloud service provider. These obligations include the audit and access rights and the security of data and systems as defined by the Solvency II Directive and the Delegated Regulation and further specified by these Guidelines.

53. The cloud outsourcing agreement between the undertaking and the cloud service provider should specify any types of activities that are excluded from potential sub-outsourcing and indicate that the cloud service provider retains full responsibility and oversight obligations for the services it has sub-outsourced.

54. The cloud outsourcing agreement should also include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-outsourcers or the sub-outsourced services that might affect the ability of the service provider to meet its responsibilities under the cloud outsourcing agreement. The notification period for those changes should be contractually pre-agreed to allow for the undertaking, at least, to carry out a risk assessment of the effects of the

proposed changes before the actual change in the sub-outsourcers or the sub-outsourced services comes into effect.

55. In case a cloud service provider plans changes to a sub-outsourcer or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, the undertaking should have the power to object to such changes and the right to terminate the contract.

Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements

56. The undertaking should monitor the performance of activities, the security measures and the adherence to the agreements of their cloud providers on an on-going basis. In order to do so, the undertaking should set up monitoring and oversight mechanisms. These include but are not limited to the management of:

a. the incidents occurred to the cloud provider with impact on the undertaking's activities;

b. data and information governance systems around the processes performed on the cloud;

c. the business continuity of the technological and supply chain;

d. the mechanisms ensuring integration of the cloud services with the systems of the undertakings; for example, the APIs (Application Programming Interface) and the user and access management process;

e. roles and responsibilities between the cloud service provider and the undertaking in relation to all the IT (including IT security and cybersecurity) and non-IT processes affected by the cloud outsourcing, which should be clearly splitted;

f. on-going and independent verifications of the Service Level Agreements, which should be agreed with the cloud service provider.

57. The undertaking should perform the activities detailed in the previous paragraph taking into account the principle of proportionality and the presence of significant sub-outsourcing, if any.

58. The AMSB should be regularly updated on the risks identified in respect of the material outsourcing. As part of this activity, undertakings should monitor and manage their concentration risk caused by cloud outsourcing arrangements.

59. In order to ensure the adequate monitoring and oversight of their cloud outsourcing arrangements, undertakings should employ enough resources with adequate skills and knowledge to monitor the services outsourced to the cloud. The undertaking's personnel in charge of these activities should have both IT and business knowledge as deemed necessary.

Guideline 15 – Termination rights and exit strategies

60. In addition to the requirements set out in the Delegated Regulation, within the cloud outsourcing agreement, at least for material outsourcing, the undertaking should have a clearly defined exit strategy clause ensuring that it is able to terminate the arrangement, where necessary. The termination should be made possible without detriment to the continuity and quality of its provision of services to policyholders. To achieve this, an undertaking should:

a. develop exit plans that are comprehensive, service based, documented and sufficiently tested where appropriate;

b. identify alternative solutions, where appropriate and feasible, and develop transition plans to enable the undertaking to remove and transfer existing activities and data from the cloud service provider to alternative service providers or back to the undertaking. These solutions should be defined with regard to the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase;

c. ensure that the cloud service provider and its significant sub-outsourcers (if applicable) adequately supports the undertaking when transferring the outsourced data, systems or applications to another service provider or directly to the undertaking; and;

d. agree with the cloud service provider that once retransferred to the undertaking, its data will be completely and irrevocably deleted by the cloud service provider.

61. When developing exit strategies, the undertaking should consider the following:

a. define objectives of the exit strategy;

b. define the trigger events (e.g. key risk indicators reporting an unacceptable level of service) that could activate the exit strategy;

c. perform a business impact analysis commensurate to the activities outsourced to identify what human and resources would be required to implement the exit plan and how much time it would take;

d. assign roles and responsibilities to manage exit plans and transition activities; and

e. define success criteria of the transition.

Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities

62. The analysis of the impacts arising from undertakings' cloud outsourcing arrangements should be performed by the supervisory authorities as part of their supervisory review process.

63. Supervisory authorities should include the supervision of undertakings' cloud outsourcing arrangements in the context of the following risks:

a. operational risk (including legal and compliance risk, outsourcing and third party management risk);

b. IT risks;

c. reputational risk; and

d. strategic risk.

64. Within their assessments, supervisory authorities should assess the following aspects on a risk-based approach:

a. appropriateness and effectiveness of undertaking's governance and operational processes related to the approval, implementation, monitoring, management and renewal of cloud outsourcing arrangements with particular focus on material outsourcing;

b. whether the undertaking has sufficient resources with adequate skills and knowledge to monitor the services outsourced to the cloud, with particular focus on material outsourcing; and

c. whether the undertaking identifies and manages all the relevant risks highlighted by these Guidelines including the concentration risk within the undertaking or the group and at country/sectoral level.

65. In case of groups, the group supervisor should ensure that the impacts of material cloud outsourcing[14] are reflected into the group supervisory risk assessment taking into account the requirements listed at the previous two paragraphs and the group specific governance and operational characteristics. In light of the above, in the context of material cloud outsourcing that involves more than one undertaking in different Member states and that is managed centrally by the parent company or by a group subsidiary (e.g. an undertaking or a group service company such as the group IT provider), the group supervisor and/or the relevant supervisory authorities of the undertakings involved in the proposed cloud outsourcing, should discuss, where appropriate, the impacts to the group risk profile of the cloud outsourcing in the context of the College of Supervisors[15].

66. In case of on-site inspections carried out at cloud service providers' premises by the supervisory authorities, without prejudice to the requirements set out in the Solvency II Directive, Guideline 31 of the EIOPA Guidelines on supervisory review process (EIOPA-BoS-14/179) and other regulatory requirements that may apply, the supervisory authorities should have the adequate mix of knowledge and experience to perform supervision of this type of requirements (such as, for example, IT and technology knowledge, IT security & cybersecurity, business continuity management, governance and third party risk management, knowledge of legal and compliance requirements of the jurisdictions where the assessment is performed).

67. Where concerns are identified that lead to the conclusion that an undertaking no longer has robust governance arrangements in place or does not comply with regulatory requirements, supervisory authorities should take appropriate actions, which may include: improving the governance arrangement, limiting or restricting the scope of the outsourced functions or requiring exit from one or more outsourcing arrangements. In particular, taking into account the need of ensuring continuity of the undertaking's operation, the cancellation of contracts could be required if the supervision and enforcement of regulatory requirements cannot be ensured by other measures.

Compliance and reporting rules

68. This document contains Guidelines issued under Article 16 of Regulation (EU) No 1094/2010. In accordance with Article 16(3) of that Regulation, competent authorities and financial institutions are required to make every effort to comply with Guidelines and Recommendations.

69. Competent authorities that comply or intend to comply with these Guidelines should incorporate them into their regulatory or supervisory framework in an appropriate manner.

70. Competent authorities need to confirm to EIOPA whether they comply or intend to comply with these Guidelines, with reasons for non-compliance, within two months after the issuance of the translated versions.

[14] The materiality of cloud outsourcing is established according to the provisions described in Guideline 7.

[15] As defined in Article 212(1) sub (e) of Directive 2009/138/EC.

71. In the absence of a response by this deadline, competent authorities will be considered as non-compliant to the reporting and reported as such.

Final provision on review

72. The present Guidelines will be subject to a review by EIOPA.

Question to stakeholders

Q15. Are the requirements set by these Guidelines and in particular by Guidelines 4 and 5 on notification and documentation requirements sufficiently proportionate? EIOPA welcomes concrete operational examples as to how to ensure that the principle of proportionality is effectively reflected in these Guidelines.

Annex I: Impact Assessment

Section 1 – Procedural issues and consultation of interested parties

In accordance with Article 16 of EIOPA Regulation, EIOPA conducts analyses of costs and benefits in the policy development process. The analysis of costs and benefits is undertaken according to an Impact Assessment methodology.

The draft Guidelines and its Impact Assessment are envisaged to be subject to a public consultation. Stakeholders' responses to public consultation will serve as a valuable input in order to revise the Guidelines.

Section 2 – Problem definition

The purchase of cloud outsourcing services falls within the broader scope of outsourcing as disciplined by Directive 2009/138/EC, Commission Delegated Regulation 2015/35 and clarified by the Section 11 EIOPA Guidelines on System of Governance.

Notwithstanding the above, given the peculiarity and specificities of cloud outsourcing, there is a lack of clear and harmonised regulatory practices across European jurisdictions on the use and management of cloud outsourcing services by insurance and reinsurance undertaking. This is the core problem that the current Guidelines aim to address with the objective to provide clearer expectations on how to apply the outsourcing provisions to the use of cloud services. Taking into account that the cloud services enable undertakings to access a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand, a unlevel playing field (e.g. with different standards and approaches adopted by the different national supervisory authorities) could have negative impacts on the prudent cloud adoption by the European (re)insurance industry. These impacts could be summarised in: potential higher costs for the undertakings that want to outsource to cloud service providers in multiple jurisdictions and potential uncoordinated supervisory practices leading to a potential unfair competition.

EIOPA identified the above mentioned needs and decided to develop specific Guidelines on outsourcing to cloud service providers in the context of the analysis performed to answer the European Commission FinTech Action plan (COM(2018) 109 final) and following interactions with several other stakeholders[16].

The work carried out by EIOPA highlighted the following main areas that need to be clarified:

- application of the regulatory definition of outsourcing[17] to the purchase of cloud services;
- risk and materiality assessment and notification to competent authorities prior to enter into a cloud outsourcing arrangements;
- management of specific risks associated to the use of cloud computing services (such as, for example: 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.

[16] Please, see footnote nr.2.

[17] Article 13 (28) of Directive 2009/138/EC.

Moreover, taking into account the work carried out by the European Banking Authority (EBA) in the fields of outsourcing and cloud outsourcing[18], another gap that the current draft Guidelines aim to address is the lack of guidance for the regulatory framework and supervisory assessment of outsourcing risks in EU insurance and reinsurance undertakings and therefore room for inconsistency in assessing outsourcing risk across jurisdictions[19] leading to a lack of comparability of supervisory practices across EU which is of crucial importance given the cross-border nature of the cloud service. Inconsistency in the treatment of potential risks related to cloud services may also lead to an unlevel playing field across jurisdictions and undertakings.

When analysing the impact from proposed policies, the impact assessment methodology foresees that a baseline scenario is applied as the basis for comparing policy options. This helps to identify the incremental impact of each policy option considered. The aim of the baseline scenario is to explain how the current situation would evolve without additional regulatory intervention.

For the analysis of the potential related costs and benefits of the proposed Guidelines, EIOPA has applied as a baseline scenario the effect from the application of the current general requirements on outsourcing in the Solvency II framework. In particular the baseline includes:

- Article 49 of the Solvency II Directive;
- Article 274 of the Solvency II Delegated Regulation;
- Section 11 of EIOPA Guidelines on system of governance.

Section 3 – Objectives pursued

The main objective of the draft Guidelines is to specify a set of principle-based rules in order to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services.

Moreover, the principle-based rules provide the supervisory authorities with a common regulatory framework and tools that should be considered as minimum European standard, in their risk assessment of risks arising from cloud outsourcing. This is further expected to lead to the harmonisation of the practices and a common level-playing field across jurisdictions.

The mentioned objectives for the Guidelines are connected to the general objectives of the Solvency II framework (deepen the integration of the EU insurance market, enhance the protection of policyholders and beneficiaries and promote better regulation) and in particular they are connected to:

- the improvement of governance and risk management for insurance and reinsurance undertakings;
- the harmonisation of supervisory methods; and

[18] Namely the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) and the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), which have been integrated into the EBA Guidelines on outsourcing and are repealed with effect from 30 September 2019.

[19] On the basis of the analysis performed by EIOPA in 2018 as part of the answer the European Commission FinTech Action plan, the current level of national guidance on cloud outsourcing for (re)insurance sector is not homogenous. For example as at 31 December 2018:

- 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.

- the promotion of compatibility of prudential supervision of insurance and banking.

The objectives of the Guidelines are also consistent with the following objectives of EIOPA, as reflected in the Regulation of the Authority:

- ensure a sound, effective and consistent level of regulation and supervision;
- ensure the taking of risks related to (re)insurance activities is appropriately regulated and supervised; and
- consumer protection.

Section 4 – Policy Options

With the aim to meet the objectives set out in the previous section, EIOPA has analysed different policy options throughout the policy development process.

The section below reflects the most relevant policy options that have been considered in relation to the different aspects associated to the cloud outsourcing process. We have also listed relevant options which have been discarded in the policy development process.

Policy issue 1: Introduction of the Guidelines versus the status quo

Policy option 1.1 Introduction of EIOPA cloud outsourcing Guidelines to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services.

Policy option 1.2 Keeping the status quo not issuing any guidance on the subject.

Policy issue 2: Development of dedicated cloud outsourcing Guidelines versus development of more detailed Guidelines on outsourcing arrangements as a whole

Policy option 2.1 Development of dedicated EIOPA cloud outsourcing Guidelines built on the current outsourcing provisions and the EBA work in the field of outsourcing.

Policy option 2.2 Development of more detailed and specific Guidelines on outsourcing arrangements which include also the specificities of Guidelines on outsourcing to cloud service providers. The Guidelines on outsourcing arrangement would build on the EBA work in the field of outsourcing.

Policy issue 3: The purchase of cloud services falls always under the scope of outsourcing versus assessment on the basis of the function outsourced

Policy option 3.1 Insurance and reinsurance undertakings should consider all the purchase of cloud services as outsourcing and then apply to all of them the regulatory requirements and these Guidelines.

Policy option 3.2: Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply. As a rule and starting point, outsourcing is assumed.

Policy issue 4: Documentation requirements

Policy option 4.1 Requiring insurance and reinsurance undertakings to document all their cloud outsourcing arrangements providing a detailed list of information to be kept (i.e. in the form of a register).

Policy option 4.2: Keep the status quo (i.e. the undertakings are free to define their own way of documenting their cloud arrangements in place).

Policy issue 5: Role for college of supervisors in the written notification process before entering into any material cloud outsourcing versus the status quo

Considering the nature of cloud services, sometimes insurance and reinsurance groups manage centrally through the parent company or another subsidiary (such as an undertaking or a group service company, e.g. the group IT provider) the design, the deployment and the monitoring of cloud services that involve more than one undertaking belonging to the group. In these cases, usually the following activities are performed centrally (short list):

- definition of business requirements,;
- materiality and risk assessment of the services outsourced and of the provider(s);
- managing and coordinating the implementation/migration activities;
- building of the service monitoring team;
- managing of the relationship with the service provider from a legal (e.g. contractual) and operational perspective.

In light of the above, in case of cross-border groups, in the context of material cloud outsourcing that involve more than one undertaking belonging to the same group and that is managed centrally by the parent company or by a group subsidiary (e.g. an undertaking or a group service company such as the group IT provider):

Policy option 5.1: giving the possibility, under certain circumstances, to insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC in the context of the College of Supervisors (i.e. one notification per group for the undertakings included in the scope of proposed cloud outsourcing).

Policy option 5.2: Requiring insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC keeping the status quo (i.e. one notification per undertaking) and recommending the supervisory authorities to make use of the College of Supervisors to supervise, in a preventive way, the impact of such type of outsourcing to the group's risk profile.

Section 5 – Analysis of impacts

Policy issue 1: Introduction of the Guidelines versus the status quo

Policy option 1.1 Introduction of EIOPA cloud outsourcing Guidelines to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services.

On the basis of the analysis performed by EIOPA to answer the European Commission FinTech Action plan, taking into account the work already performed by the EBA and the fact that some jurisdictions have issued or planned to issue guidance on cloud outsourcing, EIOPA has identified the lack of legal transparency and potential regulatory arbitrages as risks for the market participants (i.e. regulated undertakings and service

providers). Moreover, EIOPA has identified several specific risks associated to cloud outsourcing that these Guidelines aim at mitigating.

Particularly, EIOPA is the opinion that the introduction of new Guidelines on outsourcing to cloud service providers aligned to the work already performed by EBA:

a) supports the (re)insurance undertakings in their prudent transition to the cloud, providing clarity on the application of regulatory requirements, and, therefore, unlocking the opportunities that this technology provides;

b) provides a framework for cloud outsourcing for (re)insurance undertakings aligned to the one set for banking and payment institutions, enabling the scalability of the investments already made by service providers to achieve their compliance. Moreover, it gives them the possibility to provide additional services (e.g. cloud service provider compliance programs) to the industry at a fraction of the cost;

c) maximise the investments made in terms of supervisory skills and knowledge by the national supervisory authorities who supervise – in addition to the (re)insurance– the banking or the payment markets;

d) increases the protection of the policyholders in case their insurance providers uses cloud services.

In terms of cost of compliance with the Guidelines, it is reasonable to expect that the jurisdictions where the current practices overlap or show similarities with what is proposed in these draft Guidelines will bear less administrative cost both for the undertakings and the competent authorities. This is expected particularly for those jurisdictions where the insurance competent authorities are the same as those for the banking sector. In other words, the more similar are the current practices to the Guidelines the less costly will be transition is going to be. Furthermore, potential additional costs for the industry could be expected due to the chargebacks by cloud service providers to the undertakings due to the introduction of specific contracts clauses.

Policy option 1.2 Keeping the status quo not issuing any guidance on the subject.

EIOPA believes that, without the introduction of the additional guidance, the current set of Guidelines on outsourcing fail to provide an adequate regulatory framework for the insurance and reinsurance undertakings and the competent authorities in their handling of cloud outsourcing activities in the insurance and reinsurance sector.

Moreover, without the issuance of guidance on the subject the entire industry faces the risk to develop non-homogenous practices to apply the outsourcing requirements to the purchase of cloud services.

Finally, without the issuance of guidance there is the risk that negotiating non-standard contractual clauses (i.e. financial services and insurance specific clauses) with cloud service providers would be challenging in particular for smaller undertakings. This could cause higher operational risks for the entire industry with potential impacts on the policyholders (e.g. in case of wrong data or location management).

Policy issue 2: Development of dedicated cloud outsourcing Guidelines versus development of more detailed Guidelines on outsourcing arrangements as a whole

As reported above, while performing its assessment on the development of these Guidelines, EIOPA has taken into account the work carried out by the EBA in the fields of outsourcing and cloud outsourcing. Particularly, the EBA issued in 2017 their Recommendations on cloud outsourcing (EBA/REC/2017/03) and in 2019 the EBA

Guidelines on outsourcing arrangements (EBA/GL/2019/02) which have repealed the Recommendations absorbing their text.

On the basis of the results of the internal assessment mentioned in the previous paragraph, EIOPA believes that the risks arising from the usage of cloud computing by (re)insurance undertakings are, generally, aligned to the risks bear by the banking players with few minor (re)insurance specificities.

The analysis of impacts on the Policy issue nr.2 takes into account the above.

Policy option 2.1 Development of dedicated EIOPA cloud outsourcing Guidelines build on the current outsourcing provisions and the EBA work in the field of outsourcing.

Notwithstanding the fact that the purchase of cloud computing services falls within the broader scope of outsourcing, the use of cloud services has some conceptual differences from the traditional IT outsourcing. One above all is that the cloud customer does not receive from the cloud provider dedicated IT resources (such as: servers, storage or networking) as it happens in traditional IT outsourcing configurations.

The issuance of specific guidance on cloud outsourcing gives the possibility to provide clarity and homogeneity across member states on how to apply the framework on outsourcing to cloud computing while minimising the impacts on the insurance and insurance undertakings.

In order to avoid inconsistencies between the banking and the insurance sector, the Guidelines build on the:

- EBA Recommendations on cloud outsourcing (EBA/REC/2017/03) and;
- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

Policy option 2.2 Development of more detailed and specific Guidelines on outsourcing arrangements which include also the specificities of Guidelines on outsourcing to cloud service providers. The Guidelines on outsourcing arrangement would build on the EBA work in the field of outsourcing.

The issuance of new more detailed and specific Guidelines on outsourcing arrangements which include has the main benefits of: (i) keeping a consistent approach to the banking sector and (ii) minimising therefore the risk of having an additional limited implementation effort for the jurisdictions that have applied the EBA Guidelines on outsourcing also to the insurance sector.

However, the issuance of more detailed Guidelines on outsourcing arrangements built on the EBA ones, poses the risk of potential more significant implementation costs for the insurance undertakings.

Moreover, considering the market trends of expected broader and more intense use of cloud services by insurance and reinsurance undertakings, the issuance of specific guidance to ensure greater harmonization of the regulatory practices across the market on outsourcing to cloud service providers has been considered as a priority by EIOPA.

Policy issue 3: The purchase of cloud services falls always under the scope of outsourcing versus assessment on the basis of the function outsourced

Policy option 3.1 Insurance and reinsurance undertakings should consider all the purchase of cloud services as outsourcing and then apply to all of them the regulatory requirements and these Guidelines.

Considering the use of cloud services as always outsourcing provides a clear and simple framework to be applied to the purchase of cloud services and it would simplify the understanding the scope of cloud outsourcing.

However, this approach would cause additional costs to both the regulated undertakings and the service providers. Moreover, the approach under the policy option 3.1 would not be fully in line with the current market practices associated to outsourcing arrangements causing potential additional investments and running costs for the undertakings to comply with it.

In other words, although the approach under the policy option 3.1 appears to be sound to capture and manage the risks posed to the undertakings in case they decide to use cloud services, it appears to be not fully proportionate.

Policy option 3.2: Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply. As a rule and starting point, outsourcing is assumed.

Letting the undertakings to perform their own assessments to classify their purchase of cloud services as outsourcing would pose risks of lack of homogeneity among the application of the provisions across jurisdictions.

However, if complemented with clear principle-based instructions and under the presumption that outsourcing in a regulated context should be assumed, the approach under the policy option 3.2 appears to be both proportionate and sound to capture and manage the risks posed to the undertakings in case they decide to use cloud services.

Moreover, being the approach under the policy option 3.2 closer to the current practice, choosing it would result in lower costs of compliance for the regulated undertakings and the service providers.

Policy issue 4: Documentation requirements

Policy option 4.1 Requiring insurance and reinsurance undertakings to document their cloud outsourcing arrangements providing a detailed list of information to be kept (i.e. in the form of a register).

The policy option 4.1 could generate higher upfront costs for the undertakings which do not have structured approaches to manage their cloud outsourcing arrangements. However, due to the simplicity to access to the cloud and set up contractual arrangements with the cloud service providers, requiring the undertakings to document their outsourcing arrangements and keep them in a structured central register could support them in the application of sound risk management approach in the decision to outsource to cloud service providers and in the management of such services including the related concentration risks.

Furthermore, the policy option 4.1 being aligned to the approach adopted by the EBA reduces the risk of unneeded cross-sectoral differences.

Policy option 4.2: Keep the status quo (i.e. the undertakings are free to define their own way of documenting their cloud arrangements in place).

The policy option 4.2 produces lower upfront costs to set up the documentation process for the undertakings which do not have structured approaches to manage their cloud outsourcing arrangements. However, in the long run, the policy option 4.2 could produce a risk of non-homogeneity of interpretation of the requirements set by these Guidelines and the risk of unmanaged operational risks which could result in higher costs for the undertakings at a later stage.

Policy issue 5: Role for college of supervisors in the written notification process before entering into any material cloud outsourcing versus the status quo

Policy option 5.1: giving the possibility, under certain circumstances, to insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC in the context of the College of Supervisors (i.e. one notification per group).

In case of cross-border groups, in the context of material cloud outsourcing that involve more than one undertaking belonging to the same group and that is managed centrally by the parent company or by a group subsidiary (e.g. an undertaking or a group service company such as the group IT provider, giving the possibility, as an option, to perform the written notification process at the level of College of Supervisors could provide several benefits to:

- the insurance and reinsurance groups in terms, for instance, of reduced administrative burdens by performing one notification instead of several;
- the regulatory community that can have a more transparent dialogue with the experts of the group on the field of cloud computing with the possibility to share their supervisory concerns at the highest hierarchical level of the group increasing, therefore, the efficiency and effectiveness of their preventive supervision.

Furthermore, the approach described under the policy option 5.1 could increase the consistency in the supervisory practices on the subject of cloud outsourcing and IT risk management of the undertakings belonging to the group and of the group as a whole..

However, the operational feasibility of policy option 5.1 appears to be limited, particularly considering the fact that:

(i) the notification requirements for material outsourcing have been adopted in a non-homogeneous way by Member States, and

(ii) in any case, the adoption of the policy option 5.1 will not grant any exemption to the group to follow the national laws and regulations that may apply to the cloud outsourcing arrangement which would be notified to the College of Supervisors.

Policy option 5.2: requiring insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC keeping the status quo and recommending the supervisory authorities to make use of the College of Supervisors to supervise, in a preventive way, the impact of such type of outsourcing to the group's risk profile.

Taking into account the characteristics of cloud services and the activities performed in case of group-led cloud outsourcing initiatives (reported at the paragraph describing the policy option 5.1), and considering that a sound an prudent use of cloud computing is an enabler for innovation in the financial sector, keeping the status quo could have a negative impact on the adoption of the cloud for the undertakings – member of cross-border groups – established in the jurisdictions that do not constitute the first operational priority for the groups.

However, taking into account the operational limitations presented at the paragraph describing the policy option 5.1, there are risks of increasing the complexity of the cloud

computing notification process, affecting therefore the time-to-market of the re(insurance) undertakings electing to use this possibility.

Furthermore, the policy option 5.2, incorporating a specific recommendation to the supervisory community to make use of the College of Supervisors to effectively supervise the group material cloud outsourcing, appear to foster the increase of transparency and communication among the relevant supervisory authorities.

Section 6 – Comparison of options

Regarding policy options 1.1 and 1.2 on the basis of the previous section and taking into account the future trends of increasing usage of cloud services by European (re)insurers, **EIOPA has chosen the policy option 1.1** "Introduction of EIOPA cloud outsourcing Guidelines to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services". EIOPA believes that the introduction of these Guidelines could support the European insurance market risk based outsourcing to cloud service providers.

Regarding policy options 2.1 and 2.2 on the basis of the previous section and considering the preparatory analysis performed in the context of developing its answer to the European Commission FinTech Action Plan[20], **EIOPA has chosen the policy option 2.1** "Development of dedicated EIOPA cloud outsourcing Guidelines built on the current outsourcing provisions and the EBA work in the field of outsourcing" in order to, timely, answer the increasing market practices of outsourcing to cloud service providers by providing Guidelines.

Regarding policy options 3.1 and 3.2, on the basis of the previous section and with the aim of creating the minimum disruption as possible to the current practices observed in the market while, at the same time, ensuring a sound risk management of the purchase of cloud services, **EIOPA has chosen the policy option 3.2** "Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply. As a rule and starting point, outsourcing is assumed."

Considering that to keep a central repository of all cloud outsourcing arrangements and not only of those classified as material is a sound governance practice already applied by several market participants, regarding policy options 4.1 and 4.2, on the basis of the previous section, **EIOPA has chosen the policy option 4.1** "Requiring insurance and reinsurance undertakings to document their cloud outsourcing arrangements providing a detailed list of information to be kept (i.e. in the form of a register)." In any case, when evaluating the compliance to that requirement, the supervisory authorities should take particularly into account the principle of proportionality as defined by Article 29 of Solvency II Directive.

Regarding policy options 5.1 and 5.2 on the basis of the previous section and considering the potential legal and operational limitations of the policy option 5.1, , **EIOPA has chosen the policy option 5.2** "Requiring insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC keeping the status quo and recommending the supervisory authorities to make use of the College of Supervisors to supervise, in a preventive way, the impact of such type of outsourcing to the group's risk profile".

[20] Please, see footnote nr.2.

Annex II: Overview of Questions for Consultation

The questions outlined below are also included in the Template for Comments.

Q1. Is the scope of application provided appropriate and sufficiently clear?

Q2. Is the set of definitions provided appropriate and sufficiently clear?

Q3. Is the timeline to implement the Guidelines considered sufficient to ensure a smooth transition from the current operational practices to the ones provided by these Guidelines?

Q4. Is the Guideline on cloud service and outsourcing appropriate and sufficiently clear to enable the distinction between cloud services falling within the scope of outsourcing and the ones not falling within such scope?

Q5. Is the Guideline on written policy appropriate and sufficiently clear to manage the undertaking's roles, processes and procedures on outsourcing to cloud service providers? Is it consistent with the market best practices on defining the policy for general outsourcing?

Q6. Is the list of information to be notified to the national supervisory authorities considered appropriate to understand the most significant areas taken into account by the undertakings in their decision making process?

Q7. Would the introduction of a register of all cloud outsourcing arrangement have a significant impact on the current undertakings practices to manage cloud-outsourcing arrangements? What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?

Q8. Are the documentation requirements appropriate and sufficiently clear?

Q9. Taking into account the specific nature of cloud services, it has been opted to use the concept of 'materiality' to clarify, in this context, the one of 'critical or important operational function'. Is this approach appropriate and sufficiently clear?

Q10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?

Q11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?

Q12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?

Q13. Are the guideline on access and audit rights appropriate and sufficiently clear?

Q14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?

Q15. Are the requirements set by these Guidelines and in particular by Guidelines 4 and 5 on notification and documentation requirements sufficiently proportionate? EIOPA welcomes concrete operational examples as to how to ensure that the principle of proportionality is effectively reflected in these Guidelines.

Q16. Do you have any comments on the Impact Assessment?