EIOPA-BoS-20-002

Guidelines on outsourcing to cloud service providers

Table of Contents

Introduction

1. In accordance with Article 16 of Regulation (EU) No 1094/2010[1] EIOPA issues guidelines to provide guidance to insurance and reinsurance undertakings on how the outsourcing provisions set forth in Directive 2009/138/EC[2] ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/35[3] ("Delegated Regulation") needs to be applied in case of outsourcing to cloud service providers.
2. These Guidelines are based 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).
3. These Guidelines are addressed to competent authorities to provide guidance on how insurance and reinsurance undertakings (collectively "undertaking(s)") should apply the outsourcing requirements foreseen in the above mentioned legal acts in the context of outsourcing to cloud service providers.
4. The Guidelines apply to both individual undertakings and *mutatis mutandis* to groups[4].

   The entities subject to other sectoral requirements, which are part of a group, are excluded from the scope of these Guideline at solo level as they need to follow the sectoral specific requirements as well as the relevant guidance issued by the European Securities and Markets Authority and the European Banking Authority.
5. In case of intra-group outsourcing and sub-outsourcing to cloud service providers, these Guidelines should be applied in conjunction with the provisions of EIOPA Guidelines on System of Governance on intra-group outsourcing.
6. Undertakings and competent authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality[5] and the criticality or importance of the service outsourced to cloud service providers. The proportionality principle should ensure that governance arrangements, including those related to outsourcing to cloud service providers, are proportionate to the nature, scale and complexity of the underlying risks.
7. These Guidelines should be read in conjunction with and without prejudice to EIOPA Guidelines on System of Governance and to the regulatory obligations listed in paragraph 1

Definitions

8. If not defined in these Guidelines, the terms have the meaning defined in the legal acts referred to in the introduction.
9. In addition, for the purposes of these Guidelines, the following definitions apply:

[1] 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).

[2] 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, 17.12.2009, p. 1).

[3] 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).

[4] Article 212(1) of the Solvency II Directive.

[5] Article 29(3) of the Solvency II Directive.

Service provider	means a third party entity that is performing a process, service or activity, or parts thereof, under an outsourcing arrangement.
Cloud service provider	means a service provider, as defined above, responsible for delivering cloud services under an outsourcing arrangement.
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.
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.

Date of application

10. These Guidelines apply from 1 January 2021 to all cloud outsourcing arrangements entered into or amended on or after this date.

11. Undertakings should review and amend accordingly existing cloud outsourcing arrangements related to critical or important operational functions or activities with a view to ensuring compliance with these Guidelines by 31 December 2022.

12. Where the review of cloud outsourcing arrangements related to critical or important operational functions or activities is not finalised by 31 December 2022, the undertaking should inform its supervisory authority[6] of that fact, including the measures planned to complete the review or the possible exit strategy. The supervisory authority may agree with the undertaking on an extended timeline for completing that review, where appropriate.

13. The update (where needed) of the undertaking's policies and internal processes should be done by 1 January 2021 while the documentation requirements for cloud outsourcing arrangements related to critical or important operational functions or activities should be implemented by 31 December 2022.

[6] Article 13(10) of the Solvency II Directive.

Guideline 1 – Cloud services and outsourcing

14. The undertaking should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing pursuant to the Solvency II Directive. Within the assessment, consideration should be given to:

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

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

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

16. In cases where the undertaking outsources operational functions or activities to service providers which are not cloud service providers but rely significantly on cloud infrastructures to deliver their services (for example, where the cloud service provider is part of a sub-outsourcing chain), the arrangement for such outsourcing falls within the scope of these Guidelines.

Guideline 2 – General principles of governance for cloud outsourcing

17. Without prejudice to Article 274(3) of the Delegated Regulation, the undertaking's administrative, management or supervisory body ("AMSB") should ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is based on a thorough risk assessment, including all relevant risks implied by the arrangement such as information and communication technology ("ICT"), business continuity, legal and compliance, concentration, other operational risks, and risks associated to the data migration and/or the implementation phase, where applicable.

18. In case of outsourcing to cloud service providers of critical or important operational functions or activities, the undertaking, where appropriate, should reflect the changes in its risk profile due to its cloud outsourcing arrangements in its own risk and solvency assessment ("ORSA").

19. The use of cloud services should be consistent with the undertaking's strategies (for example, ICT strategy, information security strategy, operational risk management strategy) and internal policies and processes, which should be updated, if needed.

Guideline 3 – Update of the outsourcing written policy

20. In case of outsourcing to cloud service providers the undertaking should update the written outsourcing policy (for example, by reviewing it, adding a separate appendix or developing new dedicated policies) and the other relevant internal policies (for example, information security), taking into account cloud outsourcing specificities at least in the following areas:

a. the roles and responsibilities of the undertaking's functions involved, in particular AMSB, and the functions responsible for ICT, information security, compliance, risk management and internal audit;

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

cloud outsourcing arrangements related to critical or important operational functions or activities;

c. the oversight of the cloud services proportionate to the nature, scale and complexity of risks inherent in the services provided, including (i) risk assessment of cloud outsourcing arrangements and due diligence on cloud service providers, including the frequency of the risk assessment; (ii) monitoring and management controls (for example, verification of the service level agreement); (iii) security standards and controls;

d. with regard to cloud outsourcing of critical or important operational functions or activities, a reference should be made to the contractual requirements as described in Guideline 10;

e. documentation requirements and written notification to the supervisory authority regarding cloud outsourcing of critical or important operational functions or activities;

f. with regard to each cloud outsourcing arrangement that covers critical or important operational functions or activities, a requirement for a documented and, where appropriate, sufficiently tested 'exit strategy' that is proportionate to the nature, scale and complexity of the risks inherent in services provided. The exit strategy may involve a range of termination processes, including but not necessarily limited to, discontinuing, reintegrating or transferring the services included in the cloud outsourcing arrangement.

Guideline 4 - Written notification to the supervisory authority

21. The written notification requirements set in Article 49(3) of the Solvency II Directive and further detailed by EIOPA Guidelines on System of Governance are applicable to all outsourcing of critical or important operational functions and activities to cloud service providers. In case an outsourced operational function or activity previously classified as non-critical or non-important becomes critical or important, the undertaking should notify the supervisory authority.

22. The undertaking's written notification should include, taking into account the principle of proportionality, at least the following information:

a. a brief description of the operational function or activity outsourced;

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

c. the governing law of the cloud outsourcing agreement;

d. the name of the cloud 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;

e. cloud services and deployment models (i.e. public/private/hybrid/community) and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

f. a brief summary of the reasons why the outsourced operational function or activity is considered critical or important;

g. the date of the most recent assessment of the criticality or importance of the outsourced operational function or activity.

Guideline 5 – Documentation requirements

23. As part of its governance and risk management system, the undertaking should keep record of its cloud outsourcing arrangements, for example, in the form of a dedicated register kept updated over time. The undertaking should also maintain a record of terminated cloud outsourcing arrangements for an appropriate retention period subject to national regulation.

24. In case of outsourcing of critical or important operational functions or activities, the undertaking should record all of the following information:

a. the information to be notified to the supervisory authority referred to in Guideline 4;

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

c. the date of the most recent risk assessment and a brief summary of the main results;

d. the individual or decision-making body (for example the AMSB) in the undertaking that approved the cloud outsourcing arrangement;

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

f. the names of any sub-contractors to which material parts of a critical or important operational function or activity are sub-outsourced including the countries where the sub-contractors are registered, where the service will be performed and, if applicable, the locations (i.e. countries or regions) where the data will be stored;

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

h. whether the outsourced critical or important operational function or activity supports business operations that are time critical;

i. the estimated annual budget costs;

j. whether the undertaking has an exit strategy in case of termination by either party or disruption of services by the cloud service provider.

25. In case of outsourcing of non-critical or non-important operational functions or activities, the undertaking should define the information to be recorded on the basis of the nature, scale and complexity of the risks inherent in the services provided by the cloud service provider.

26. The undertaking should make available to the supervisory authority, on request, all information necessary to enable the supervisory authority to perform supervision of the undertaking, including a copy of the outsourcing agreement.

Guideline 6 – Pre-outsourcing analysis

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

a. assess if the cloud outsourcing arrangement concerns a critical or important operational function or activity in accordance with Guideline 7;

b. identify and assess all relevant risks of the cloud outsourcing arrangement in accordance with Guideline 8;

c. undertake appropriate due diligence on the prospective cloud service provider in accordance with Guideline 9;

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 – Assessment of critical or important operational functions and activities

28. Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing arrangement relates to an operational function or activity that is critical or important. In performing such an assessment, where relevant, the undertaking should consider whether the arrangement has the potential to become critical or important in the future. The undertaking should also reassess the criticality or importance of the operational function or activity previously outsourced to cloud service providers, if the nature, scale and complexity of the risks inherent in the agreement materially changes.

29. In the assessment, the undertaking should take into account, together with the outcome of the risk assessment, at least, the following factors:

a. the potential impact of any material disruption to the outsourced operational function or activity or failure of the cloud service provider to provide the services at the agreed service levels on the undertaking's:

   i. continuous compliance with its regulatory obligations;

   ii. short and long-term financial and solvency resilience and viability;

   iii. business continuity and operational resilience;

   iv. operational risk, including conduct, ICT and legal risks;

   v. reputational risks.

b. the potential impact of the cloud outsourcing arrangement on the ability of the undertaking to:

   i. identify, monitor and manage all relevant risks;

   ii. comply with all legal and regulatory requirements;

   iii. conduct appropriate audits regarding the operational function or activity outsourced.

c. the undertaking's (and/or group's where applicable) aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same business area;

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

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

f. the protection of personal and non-personal data and the potential impact on the undertaking, policyholders or other relevant subjects of a confidentiality breach or failure to ensure data availability and integrity based on *inter alia* Regulation (EU) 2016/679[7]. The undertaking should particularly take into

[7] 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).

consideration data that is business secret and/or sensitive (for example, policyholders' health data).

Guideline 8 – Risk assessment of cloud outsourcing

30. In general, the undertaking should adopt an approach proportionate to the nature, scale and complexity of the risks inherent in the services outsourced to cloud service providers. This includes, assessing the potential impact of any cloud outsourcing, in particular, on their operational and reputational risks.

31. In case of outsourcing of critical or important operational functions or activities to cloud service providers, an undertaking should:

a. take into account the expected benefits and costs of the proposed cloud outsourcing arrangement, including weighing 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.

b. assess, where applicable and appropriate, the risks, including legal, ICT, compliance and reputational risks, and the oversight limitations arising from:

   i. the selected cloud service and the proposed deployment models (i.e. public/private/hybrid/community);

   ii. the migration and/or the implementation;

   iii. the activities and related data and systems which are under consideration to be outsourced (or have been outsourced) and their sensitivity and required security measures;

   iv. the political stability and the security situation of the countries (within or outside the EU) where the outsourced services are or may be provided and where the data are or are likely to be stored. The assessment should consider:

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

      2. the law enforcement provisions in place;

      3. the insolvency law provisions that would apply in the event of a service provider's failure and any constrains that would arise with regard to the urgent recovery of the undertaking's data;

   v. sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the cloud service provider and the risk that long and complex chains of sub-outsourcing reduce the ability of the undertaking to oversee its critical or important operational functions or activities and the ability of supervisory authorities to effectively supervise them;

   vi. the undertakings overall concentration risk to the same cloud service provider, including outsourcing to a cloud service provider that is not easily substitutable or multiple outsourcing arrangements with the same cloud service provider. When assessing the concentration risk, the undertaking (and/or the Group, where applicable) should take into account all its cloud outsourcing arrangements with that cloud provider.

32. The risk assessment should be performed before entering into a cloud outsourcing. If the undertaking becomes aware of significant deficiencies and/or significant changes to the services provided or to the situation of the cloud service

provider, the risk assessment should be promptly reviewed or re-performed. In case of renewal of a cloud outsourcing arrangement concerning its content and scope (for example, enlargement of the scope or inclusion in the scope of critical or important operational functions previously not included), risk assessment should be re-performed.

Guideline 9 – Due diligence on cloud service provider

33. The undertaking should ensure in its selection and assessment process that the cloud service provider is suitable according to the criteria defined by its written outsourcing policy.

34. The due diligence on the cloud service provider should be performed prior to outsourcing any operational function or activity. In case the undertaking enters into a second agreement with a cloud service provider that has already been assessed, the undertaking should determine, on a risk-based approach, whether a second due diligence is needed. If the undertaking becomes aware of significant deficiencies and/or significant changes of the services provided or the situation of the cloud service provider, the due diligence should be promptly reviewed or re-performed.

35. In case of cloud outsourcing of critical or important operational functions, the due diligence should include an evaluation of the suitability of the cloud service provider (for example, skills, infrastructure, economic situation, corporate and regulatory status). Where appropriate, the undertaking can use to support the due diligence performed evidence, certifications based on international standards, audit reports of recognised third parties or internal audit reports.

Guideline 10 – Contractual requirements

36. 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.

37. Without prejudice to the requirements defined in Article 274 of the Delegated Regulation, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the undertaking and the cloud service provider should set out:

a. a clear description of the outsourced function to be provided (cloud services, including the type of support services);

b. the start date and end date, where applicable, of the agreement and the notice periods for the cloud service provider and for the undertaking;

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

d. the parties' financial obligations;

e. whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof) is permitted, and, if so, the conditions to which the significant sub-outsourcing is subject to (see Guideline 13);

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

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

h. the right for the undertaking to monitor the cloud service provider's performance on a regular basis;

i. the agreed service levels which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

j. the reporting obligations of the cloud service provider to the undertaking, including, as appropriate, the obligations to submit reports relevant for the undertaking's security function and key functions, such as reports of the internal audit function of the cloud service provider;

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

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

m. the requirement for the cloud service provider to grant the undertaking, its supervisory authorities and any other person appointed by the undertaking or the supervisory authorities, the following:

    i. full access to all relevant business premises (head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the cloud service provider's external auditors ("access rights");

    ii. unrestricted rights of inspection and auditing related to the cloud outsourcing arrangement ("audit rights"), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements;

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.

Guideline 11 – Access and audit rights

38. The cloud outsourcing agreement should not limit the undertaking's effective exercise of access and audit rights as well as control options on cloud services in order to fulfil its regulatory obligations.

39. 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.

40. In determining the frequency and the scope of its exercise of access or audit rights, the undertaking should consider whether the cloud outsourcing is related to a critical or important operational function or activity, the nature and extent of risk and impact on the undertaking from the cloud outsourcing arrangements.

41. If the exercise of its access or audit rights, or the use of certain audit techniques creates a risk for the environment of the cloud service provider and/or another cloud service provider's client (for example, the 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 and service to the undertaking (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the cloud service provider).

42. 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 organisational 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), or pooled audits performed by a third-party appointed by them.

43. In case of cloud outsourcing of critical or important operational functions or activities, undertakings should make use of the method referred to in paragraph 42(a) only if they:

a. ensure that the scope of the certification or the audit report covers the systems (for example, processes, applications, infrastructure, data centres, etc.) and the controls identified by the undertaking and assesses the compliance with relevant regulatory requirements;

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

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

d. are satisfied with the aptitude of the certifying or auditing party (for example, with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);

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

f. 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;

g. retain the contractual right to perform individual on-site audits at their discretion with regard to the cloud outsourcing of critical or important operational functions or activities; such right should be exercised in case of specific needs not possible through other types of interactions with the cloud service provider.

44. For outsourcing to cloud service providers of critical or important operational functions, the undertaking should assess whether third-party certifications and reports as referred to in paragraph 42(a) are adequate and sufficient to comply with its regulatory obligations and, on a risk based approach, should not rely solely on these reports and certificates over time.

45. Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third-party acting on behalf of the undertaking(s)) should provide prior notice in a reasonable time period, unless an early prior notification has not been possible due to an emergency or crisis situation. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit.

46. 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 the relevant audits and/or assessments.

Guideline 12 – Security of data and systems

47. The undertaking should ensure that cloud service providers comply with European and national regulations as well as appropriate ICT security standards.

48. In case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking should additionally define specific information security requirements in the outsourcing agreement and monitor compliance with these requirements on a regular basis.

49. For the purposes of paragraph 48, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking, applying a risk based approach, and taking into account its responsibilities and the ones of the cloud service provider, should:

a. agree on clear roles and responsibilities between the cloud service provider and the undertaking in relation to the operational functions or activities affected by the cloud outsourcing, which should be clearly split;

b. 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;

c. consider specific measures, where necessary, for data in transit, data in memory and data at rest, for example, the use of encryption technologies in combination with an appropriate keys management;

d. consider the mechanisms of integration of the cloud services with the systems of the undertakings, for example, the Application Programming Interfaces and a sound user and access management process;

e. contractually ensure that network traffic availability and expected capacity meet strong continuity requirements, where applicable and feasible;

f. define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain, where applicable;

g. have a sound and well documented incident management process including the respective responsibilities, for example, by the definition of a cooperation model in case of actual or suspected incidents occur;

h. adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations;

i. monitor the fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms implemented by the cloud service provider that would mitigate the risks related to the provided services.

Guideline 13 – Sub-outsourcing of critical or important operational functions or activities

50. If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should:

a. specify any types of activities that are excluded from potential sub-outsourcing;

b. indicate the conditions to be complied with in case of sub-outsourcing (for example, that the sub-outsourcer will also fully comply with the relevant obligations of the cloud service provider). These obligations include the audit and access rights and the security of data and systems;

c. indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced;

d. include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement. The notification period for those changes should allow 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;

e. ensure, in cases where 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, that the undertaking has the right to object to such changes and/or the right to terminate and exit the contract.

Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements

51. The undertaking should monitor, on a regular basis, the performance of activities, the security measures and the adherence to agreed service level by their cloud service providers on a risk based approach. The main focus should be on the cloud outsourcing of critical and important operational functions.

52. In order to do so, the undertaking should set up monitoring and oversight mechanisms, which should take into account, where feasible and appropriate, the presence of sub-outsourcing of critical or important operational functions or a part thereof.

53. The AMSB should be periodically updated on the risks identified in the cloud outsourcing of critical or important operational functions or activities.

54. 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 ICT and business knowledge as deemed necessary.

Guideline 15 – Termination rights and exit strategies

55. In case of cloud outsourcing of critical or important operational functions or activities, within the cloud outsourcing agreement 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, the undertaking should:

a. develop exit plans that are comprehensive, service based, documented and sufficiently tested (for example, by carrying out an analysis of the potential costs, impacts, resources and timing implications of the various potential exit options);

b. identify alternative solutions and develop appropriate and feasible 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, taking the necessary measures to ensure business continuity during the transition phase;

c. ensure that the cloud service provider adequately supports the undertaking when transferring the outsourced data, systems or applications to another service provider or directly to the undertaking;

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

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

a. define objectives of the exit strategy;

b. define the trigger events (for example, 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 other 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;

e. define success criteria of the transition.

Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities

57. The supervisory authorities should perform the analysis of the impacts arising from undertakings' cloud outsourcing arrangements as part of their supervisory review process. The analysis of the impacts should focus, in particular, on the arrangements related to the outsourcing of critical or important operational functions or activities.

58. Supervisory authorities should consider the following risks in the supervision of undertakings' cloud outsourcing arrangements:

a. ICT risks;

b. other operational risks (including legal and compliance risk, outsourcing and third party management risk);

c. reputational risk;

d. concentration risk, including at country/sectoral level.

59. Within their assessment, supervisory authorities should include 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;

b. whether the undertaking has sufficient resources with adequate skills and knowledge to monitor the services outsourced to the cloud;

c. whether the undertaking identifies and manages all risks highlighted by these Guidelines.

60. In case of groups, the group supervisor should ensure that the impacts of cloud outsourcing of critical or important operational functions or activities are reflected in the group supervisory risk assessment, taking into account the requirements listed in paragraphs 58-59 and the group's individual governance and operational characteristics.

61. If cloud outsourcing of critical or important operational functions or activities involves more than one undertaking in different Member states and is managed centrally by the parent company or by a group subsidiary (for example, an undertaking or a group service company such as the group ICT provider), the group supervisor and/or the relevant supervisory authorities of the undertakings involved in the cloud outsourcing, should discuss, where appropriate, the impacts of cloud outsourcing to the group risk profile in the College of Supervisors.

62. 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, for example, requiring the undertaking to improve the governance arrangement, limiting or restricting the scope of the outsourced functions or requiring to 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 supervision and enforcement of regulatory requirements could not be ensured by other measures.

Compliance and reporting rules

63. 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.

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

65. 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.

66. 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

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