MILLIMAN BRIEFING NOTE

EIOPA's guidance on cloud outsourcing

Checklist for outsourcing to the cloud

Claire Booth, FIA, CERA
Tanya Hayward, FIA
Peter Moore, FIA
Tom Peplow, MSc

Milliman

Overview

Cloud services can provide undertakings with several benefits: greater economies of scale, flexibility, operational efficiencies, productivity, global reach and cost-effectiveness. However, these arrangements need to be entered into with care to ensure that the risks that arise as a result of them are identified and managed appropriately. For example, data protection, security issues and concentration risk may be concerns (from the point of view of individual undertakings as well as at an industry level, as large cloud service providers can become a single point of failure). That being said, cloud adoption as part of a holistic digital transformation could be the force multiplier required to propel insurers forward in a rapidly evolving digital world.

On 1 July 2019, the European Insurance and Occupational Pension Authority (EIOPA) launched a consultation on guidelines on outsourcing to cloud service providers.[1] These guidelines (which are addressed to insurance undertakings, reinsurance undertakings and national supervisory authorities) provide guidance on how the outsourcing provisions, set forth in the Directive 2009/138/EC,[2] in the Commission's Delegated Regulation 2015/35[3] and in EIOPA's Guidelines on System of Governance,[4] need to be applied in the case of outsourcing to cloud service providers.

The guidelines will apply from 1 July 2020 to all cloud outsourcing arrangements entered into or amended on or after this date. Undertakings are advised to review and amend their existing cloud outsourcing arrangements and ensure they are compliant with the Guidelines by 1 July 2022. Undertakings that have not finalised their reviews of material cloud outsourcing arrangements by 1 July 2022 will need to inform their supervisory authorities along with information on the measures they have planned to complete their reviews or possible exit strategies.

The guidelines define cloud services as '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").'

EIOPA has developed the guidelines with the following stated objectives:

- To provide clarification and transparency to market participants avoiding potential regulatory arbitrages
- To foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing

When developing these guidelines EIOPA also considered the most recent guidance published by the European Banking Authority (EBA)[5] recognising the potential risks of regulatory fragmentation and knowing that the main associated risks are similar across the financial sectors.

Implications for firms

EIOPA's guidelines on outsourcing give a strong indication as to the extent to which provision of cloud services by outsourcers should be assessed, managed and reviewed. In many ways the message here is that outsourcing is not at all the 'easy option,' and in recognition of this fact cost-benefit analysis should be carried out to ensure that it is the right option for the firm.

The paper goes into a high level of detail in prescribing the areas which should be assessed before, during and after embarking on an outsourcing agreement with a cloud provider. As a first step, undertakings are advised to establish whether their cloud service provider arrangements fall under the definition of outsourcing.[6] We expect that this will provide some work and indeed challenges for firms to implement initially. For example, some of the guidelines encourage firms to identify the characteristics of the outsourcing arrangement, but do not

[1] EIOPA (1 July 2019). Consultation Paper on the Proposal for Guidelines on Outsourcing to Cloud Service Providers. Retrieved 23 October 2019 from https://eiopa.europa.eu/Publications/Consultations/2019-07-01%20ConsultationDraftGuidelinesOutsourcingCloudServiceProviders.pdf.

[2] The full text is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:335:0001:0155:en:PDF.

[3] The full text is available at http://publications.europa.eu/resource/cellar/e0c803af-9e0f-11e4-872e-01aa75ed71a1.0006.03/DOC_477.

[4] The full text is available at https://eiopa.europa.eu/publications/eiopa-guidelines/guidelines-on-system-of-governance.

[5] EBA (25 February 2019). Final Report EBA/GL/2019/02: EBA Guidelines on Outsourcing Arrangements. Retrieved 23 October 2019 from https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.

[6] Outsourcing is defined as: 'An arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself' under Article 13(28) of the Solvency II Directive.' See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0138&from=EN.

provide any guidance on the consequences or significance of these characteristics. The firm will therefore need to assess the significance in terms of ongoing risk management and monitoring of the outsourcing arrangement. This is applicable to factors such as deciding whether the function is provided on an ongoing or recurrent basis, and establishing whether the outsourcing arrangement is material or not.

EIOPA's advice follows a general pattern of regulatory interest in the area of operational resilience when it comes to outsourcing and cloud use. The Bank of England's July 2018 Discussion Paper[7] highlights that the increased use of outsourcing results in concentration risks, given the reliance on a small number of technology providers. The paper suggests that firms should have thorough knowledge of the new risks that arise as a result of this increased reliance, through a comprehensive understanding and mapping of the systems and processes that support their business services. Additionally, the oversight by boards and senior management needs to cover any activities outsourced to third-party providers, including cloud service providers. Executive sponsorship should be given to define a clear digital strategy which goes beyond a cloud 'lift and shift,' alongside cultivating internal talent capable of keeping pace with technology innovations and the associated emerging risks.

Furthermore, the Financial Conduct Authority (FCA) also released Finalised Guidance (FG) 16/5 on cloud outsourcing in September 2019[8] in a similar vein to the EIOPA paper. Much like the EIOPA guidelines, the FCA guidance stresses that firms should identify whether the outsourcing arrangement is material, identify and manage the risks associated with the outsourcing arrangement and develop an outsourcing exit plan. The FCA also highlights the need to manage complex relationships in outsourcing supply chains.

IT considerations

Information technology (IT) should have a clear part to play in implementing EIOPA's advice. A mature IT organisation will have embedded processes for handling procurement decisions. These existing processes can be extended to consider the implications of dependencies on cloud service providers and the interdependencies between service providers, which may adversely affect service availability.

IT can support the business by establishing a coherent cloud strategy, particularly for PaaS and IaaS offerings. A key consideration with cloud adoption is balancing economies of scale with spreading of risk. There are considerable advantages to having a strategic partnership with a single vendor, which extend beyond price leverage. Spreading services across vendors can reduce risk at the cost of increased operational complexity and reduced value in each relationship. A hybrid cloud[9] strategy may help reduce operational complexity whilst mitigating risks specific to public cloud offerings.

With many vertical solutions being delivered as SaaS, business units are able to work around IT and acquire a service directly with a vendor. Moving service acquisition closer to the business has benefits. However, isolated decisions may have unintended consequences. It is important to ensure that a governance framework exists that reaches beyond IT procurement decisions. Done well, IT can facilitate this process, providing expertise not present in each business unit.

Firms might also want to consider difficulties which may be encountered when exiting a cloud arrangement. In practice, off-boarding of data and/or finding an equivalent capability could be challenging. Before exiting a cloud solution, consideration should be given to the availability of alternative solutions, the cost of these alternatives, the cost and time involved in migration and the level of transition risk. The more difficult it is to change providers, the more due diligence is required during acquisition.

Checklist

Given the level of requirements before, during and after embarking on an outsourcing agreement, we have prepared a checklist that outlines what steps undertakings need to complete when initiating, maintaining and renewing, terminating or substituting cloud service provider agreements. This checklist should be read in conjunction with the EIOPA guidelines on outsourcing to cloud service providers as well as relevant parts of the Solvency II Directive[10] and Delegated Regulation.

EIOPA also specifies that supervisory authorities will carry out analysis of impacts as part of the supervisory review process in the context of operational risks, IT risks, reputational risks and strategic risks. Guideline 16 sets out further details on supervisory assessment, but we have not included it in the checklist below as the requirement does not relate to actions firms are required to carry out.

We hope that undertakings find this checklist to be a useful tool for managing their cloud service provider agreements.

[7] Bank of England (July 2018). Discussion Paper: Building the UK Financial Sector's Operational Resilience. Retrieved 23 October 2019 from https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A.

[8] FCA (September 2019). FG 16/5 Guidance for Firms Outsourcing to the 'Cloud' and Other Third-Party IT Services. Retrieved 23 October 2019 from https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf.

[9] A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them.

[10] Directive 2009/138/EC, op cit.

Undertaking checklist for managing cloud service provider agreements

A. BEFORE CONTRACT INITIATION

FIGURE 1: UNDERTAKING CHECKLIST FOR MANAGING CLOUD SERVICE PROVIDER AGREEMENTS, AT CONTRACT INITIATION

EIOPA GUIDELINE NO.	GUIDELINE REFERENCE	CHECKLIST ITEM	STATUS
1	**Cloud services and outsourcing**	▪ Establish whether cloud service should be classified as outsourcing as per the definition in article 13(28)11 of the Solvency II Directive.	
		– Establish whether outsourced function is performed on recurrent or ongoing basis.	
		– Establish whether outsourced function would or could be performed in the course of regular business actions.	
		▪ Consider all aspects of arrangement if it covers multiple functions.	
		▪ Identify, measure, monitor, manage and report risks caused by arrangements with third parties, regardless of whether or not the third parties are cloud service providers (taking into account proportionality and materiality of outsourced function).	
2	**General principles of governance for cloud outsourcing**	▪ Undertaking's administrative, management or supervisory body (AMSB) to decide whether to enter into material outsourcing agreement, based on thorough risk assessment.	
		▪ Where appropriate, reflect changes in risk profile due to arrangement in own risk and solvency assessment (ORSA).	
		▪ Ensure use of cloud services is consistent with strategies and internal policies and processes.	
4	**Written notification to the supervisory authority**	▪ Ensure that a written notification is submitted to the supervisory authority for material cloud outsourcing arrangements.	
		▪ Ensure that the written notification complies with the EIOPA guidelines on System of Governance (Guideline 64[12]), Article 49(3) of Solvency II Directive and EIOPAs guidelines on outsourcing to cloud service providers.	
6	**Pre-outsourcing analysis**	Before entering into any cloud outsourcing arrangement, the following should be addressed: ▪ Assess whether cloud outsourcing arrangement is material, according to factors included in Guideline 7.	
		▪ Identify and assess all[13] relevant risks of cloud outsourcing arrangement.	
		▪ Undertake appropriate due diligence[14] on prospective cloud service provider.	
		▪ Identify and assess conflicts of interest that the outsourcing may cause in line with the requirements set out in Article 274 (3) (b)[15] of the Delegated Regulation.	
7	**Materiality assessment**	▪ Assess whether cloud outsourcing has to be considered 'material,' according to factors included in **Guideline 7** (also addressed in Guideline 6).	

[11] '"Outsourcing" means an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself.'

[12] 'In its written notification to the supervisory authority of any outsourcing of critical or important functions or activities the undertaking should include a description of the scope and the rationale for the outsourcing and the service provider's name. When outsourcing concerns a key function, the information should also include the name of the person in charge of the outsourced function or activities at the service provider.'

[13] In our opinion, this should be carried out by the first line with independent challenge from the second line.

[14] Guideline 9 offers some indication of areas which should be considered as part of due diligence.

[15] '...the service provider has adopted all means to ensure that no explicit or potential conflict of interests jeopardize the fulfilment of the needs of the outsourcing undertaking.'

EIOPA GUIDELINE NO.	GUIDELINE REFERENCE	CHECKLIST ITEM	STATUS
8	**Risk assessment of cloud outsourcing**	▪ Assess potential impact of material outsourcing on operational, strategic, concentration and reputational risk, and make use of scenario analysis.	
		▪ Carry out cost-benefit analysis.	
		▪ Carry out a risk assessment including the items in point 30 of Guideline 8.	
9	**Due diligence on cloud service provider**	▪ Perform due diligence, applying criteria defined by written outsourcing policy and include evaluation of: – Suitability of cloud provider – Evidence/certificates based on common standards	
10	**Contractual requirement**	▪ Set out rights and obligations for the firm and the cloud service provider in a written agreement, using the requirements laid out in Article 274 of the Delegated Regulation, Article 38 of the Solvency II Directive and point 35 of Guideline 10.	
11	**Access and audit rights**	▪ Ensure that outsourcing agreement does not limit undertaking's information, access and audit rights as well as does control options on cloud services in order to fulfil its regulatory obligations.	
		▪ Ensure that undertaking receives information it needs to adequately manage and monitor risks associated with cloud outsourcing arrangements.	
12	**Security of data and systems**	▪ Ensure cloud service providers comply with appropriate[16] IT security and data protection standards.	
		▪ Define data and system security requirements in the outsourcing agreement.	
		▪ Consider the specific requirements set out in Guideline 12 regarding the results of the risk assessment performed in accordance with Guideline 8.	
13	**Sub-outsourcing**	▪ Specify in cloud outsourcing agreement whether or not sub-outsourcing of critical undertaking functions is permitted or expressly excluded.	
		▪ Ensure that sub-outsourcer will fully comply with obligations existing between undertaking and cloud service provider.	
		▪ Ensure cloud outsourcing agreement specifies any types of activities that are excluded from potential sub-outsourcing and indicates that cloud service provider retains full responsibility for services it has sub-outsourced.	
		▪ Ensure cloud outsourcing agreement includes obligation for cloud service provider to inform undertaking of any planned significant changes to sub-outsourcers or sub-outsourced services.	
		▪ Pre-agree notification period for above-mentioned changes.	
		▪ Ensure ability exists to object to changes and terminate contract if changes would have an adverse effect on the risk assessment of the agreed services.	
15	**Termination rights and exit strategies**	▪ Include clearly defined exit strategy in agreement and ensure ability to terminate arrangement where necessary for material outsourcing.	
		▪ Ensure that termination is possible without detriment to the continuity and quality of service provision to policyholders. Points 60 and 61 of Guideline 15 list actions that undertakings should take to achieve this and considerations for developing an exit strategy.	

[16] In our opinion, these standards should be those which are defined by the company in its governance framework (as opposed to reliance on an external standard alone).

B. AT CONTRACT INITIATION/DURING CONTRACT TERM

FIGURE 2: UNDERTAKING CHECKLIST FOR MANAGING CLOUD SERVICE PROVIDER AGREEMENTS, DURING CONTRACT TERM

EIOPA GUIDELINE NO.	GUIDELINE REFERENCE	CHECKLIST ITEM	STATUS
1	**Cloud services and outsourcing**	▪ Identify, measure, monitor, manage and report` risks due to relationships with third parties (regardless of whether or not those third parties are cloud service providers).	
2	**General principles of governance for cloud outsourcing**	▪ Reflect changes on risk profile within the ORSA.	
		▪ Update internal policies and processes, if needed.	
3	**Written policy on outsourcing to cloud service providers**	▪ Update written outsourcing policy to take into account cloud computing specificities.	
5	**Documentation requirements**	▪ Update register to include all material and nonmaterial functions outsourced to cloud service providers and maintain information for an appropriate retention period.	
		▪ Be prepared to provide supervisory authority with register, copy of outsourcing agreement and related information on periodical assessment on request.	
8	**Risk assessment of cloud outsourcing**	▪ Carry out risk assessment on periodical basis, and before renewal, as defined in written policy.	
		▪ Carry out risk assessment on deficiencies or significant changes to the services provided or to the service provider.	
11	**Access and audit rights**	▪ Exercise access and audit rights, determine audit frequency and areas and services to be audited on risk-based approach, according to Section 8 of EIOPA Guidelines on System of Governance.	
		▪ Include assessments of the security and control environment of service provider (and any sub-outsourcer) in scope of audits, along with the incident management process and the undertaking's observance of these guidelines in relation to cloud outsourcing arrangements.	
		▪ Consider nature and extent of risk and the impact on the undertaking from cloud outsourcing arrangements to determine frequency of audit assessment.	
		▪ Agree alternative ways to obtain assurances from cloud service provider if performance of audits or 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.	
		▪ Determine whether it is appropriate to use third-party certifications and third-party or internal audit reports made available by cloud service provider.	
		▪ Determine whether it is appropriate to use pooled audits (i.e., performed jointly with other clients of the same cloud service provider), audits performed by third-party clients or by another party appointed by them.	
		▪ Before a planned on-site visit, ensure prior notice is provided in a reasonable period.	
		▪ Verify that staff performing the audit or reviewing third-party certification or service provider's audit reports have the appropriate skills and knowledge.	
12	**Security of data and systems**	▪ Monitor compliance with system security requirements on an ongoing basis.	
		▪ Periodically review data residency policy with the cloud service provider.	

EIOPA GUIDELINE NO.	GUIDELINE REFERENCE	CHECKLIST ITEM	STATUS
14	**Monitoring and oversight of cloud outsourcing arrangement**	▪ Monitor performance of activities, security measures and adherence to agreements of cloud providers on an ongoing basis, taking into account proportionality and the presence of significant sub-outsourcing.	
		▪ Update AMSB regularly on risks identified in respect of material outsourcing.	
		▪ Monitor and manage concentration risk caused by cloud outsourcing agreements.	
		▪ Ensure enough staff resources with adequate skills and knowledge are available to monitor services outsourced to the cloud.	

How Milliman can help

Our deep expertise in risk management derives from our cutting-edge research and practical experience working with clients to assist them with their risk management and modelling needs. Our clients know that they can have confidence in us to provide excellent service and innovative, effective and dynamic solutions that fully meet their needs. We don't believe that all companies are the same, so our approach enables us to ensure that the solution each client receives is tailored to their precise circumstances and maturity levels.

In the operational resilience area, we offer assistance with:

- Review of existing risk management frameworks
- Gap analysis review
- Development of risk appetite statements and articulating them in terms of impact tolerances
- Design and building of operational risk models to facilitate understanding and quantification of the risk
- Development of risk management frameworks which improve operational resilience

If you have any questions or comments on this paper, or on any other issues affecting operational resilience, please contact any of the consultants below or your usual Milliman consultant.

Milliman

Milliman is among the world's largest providers of independent consulting. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

Milliman maintains a strong and growing presence in Europe with over 350 professional consultants serving clients from offices in Amsterdam, Brussels, Bucharest, Dublin, Dusseldorf, London, Madrid, Milan, Paris, Warsaw, and Zurich.

uk.milliman.com

CONTACT

United Kingdom

Claire Booth
claire.booth@milliman.com

Tanya Hayward
tanya.hayward@milliman.com

Peter Moore
peter.moore@milliman.com

Tom Peplow
tom.peplow@milliman.com