Guidelines on outsourcing to cloud service providers. International Bulletin, March 2021.

The growing importance of cloud service providers (CSPs) reflects the benefits they have brought to businesses and, in turn, to investors by reducing costs as well as increasing efficiency and operational flexibility. However, using these providers poses a number of challenges in terms of location and data protection, as well as giving rise to potential security problems and concentration risks, which, if not properly dealt with, could threaten investor protection, market integrity and financial stability.In this regard, on 3 June 2020, ESMA published a consultation paper (CP) containing its draft guidelines. Subsequently, on 18 December 2020, it published the final report on the guidelines, which will apply to new agreements entered into from 31 July 2021 and to older agreements amended or renewed on or after that date. Other existing agreements must be adjusted to comply with the provisions of these guidelines by 31 December 2022.
The draft guidelines are intended to help firms and competent authorities to identify, address and monitor the risks and challenges that arise during the process that takes place when entering into agreements with CSPs.

The guidelines apply to the competent authorities and collective investment institutions (AIF management companies and the depositories of these funds, UCITS and management companies and depositories of UCITS, or investment companies when no management company has been appointed), central counterparties (including Tier 2 third-country companies), central securities depositories (CSDs), trade repositories (TRs), investment firms and credit institutions that provide investment services, credit rating agencies, market operators of trading venues, data supply service providers, critical benchmark administrators and securitisation repositories.

The purpose of these guidelines is to establish consistent, efficient and effective supervisory practices within the European System of Financial Supervision (ESFS) and to ensure the common, uniform and consistent application of the requirements. For this purpose, a key definition relating to outsourcing is included, namely, the definition of what a critical or important outsourced function should be: any function whose defect or failure in its performance would materially impair a firm’s compliance with its obligations under the applicable legislation, a firm’s financial performance or the soundness or the continuity of a firm’s main services and activities.

A description of each guideline included in the Final Report accompanied by an observation on its treatment in the consultation process is provided below:

Guideline 1. Governance, oversight and documentation

Guideline 1 provides that a firm must have an accurate and up-to-date cloud outsourcing strategy that is consistent with its internal strategy, policies and procedures.The responsibilities for documentation, management and control must be clearly defined by the firm and sufficient resources allocated to ensure compliance. Additionally, a firm should either establish an oversight function or appoint a senior staff member who is directly accountable to the management body and responsible for managing and overseeing the risks of cloud outsourcing arrangements – particularly in the case of critical or important functions, which must be reassessed periodically, and whenever there are substantial changes. In any case, firms should take into account the nature, scale and complexity of their business, including in terms of risk for the financial system.

Small and less complex firms should at least ensure a clear division of tasks and responsibilities for the management and control of cloud outsourcing arrangements.
The firms should also maintain an updated register of information on all its cloud outsourcing arrangements with the CSP, distinguishing between the outsourcing of critical functions and other outsourcing arrangements.
On this question, respondents were broadly in agreement with ESMA's risk-based approach and focus on critical or important functions. However, comments were received requesting further guidance on the definitions of key terms and pointing out the need to ensure consistency with the EBA guidelines[1] in this matter, given the possible interactions between the two regulatory developments for firms falling within the scope of both sets of guidelines. ESMA's response was that given the wide range of firms within the scope of the guidelines, it does not believe that it is useful to be more prescriptive in the text as the guidelines already provide definitions that are consistent with the MiFID framework and its amendments. Lastly, it stressed that ESMA has been careful to ensure consistency with the EBA and EIOPA guidelines[2]. In addition, ESMA is mindful of the proposal for a Regulation on Digital Operational Resilience of the EC (DORA)[3] and the IOSCO consultation on new principles on outsourcing[4].

Guideline 2. Pre-outsourcing analysis and due diligence

Guideline 2 addresses the assessment of the potential provider and framework of action prior to signing any cloud outsourcing arrangement. Specifically, it requires the firm to assess whether critical functions are to be outsourced, identify the risks that may arise from the cloud outsourcing arrangement, undertake appropriate due diligence on the prospective CSP, and identify and assess the possible conflicts of interest that the outsourcing may cause. However, the principle of proportionality also applies in this guideline, stating that the pre-outsourcing analysis and due diligence should be proportionate to the nature, scale and complexity of the function that the firm intends to outsource and the risks inherent to this function. Although it does specify that it must include at least an assessment of the potential impact of the cloud outsourcing arrangement on the firm's operational, legal, compliance, and reputational risks.Specifically, if the arrangement involves critical functions, the firm should assess all relevant risks that may arise as a result of the cloud outsourcing arrangement, including risks in relation to information and communication technology, information security, business continuity, legal and compliance, reputational risks, operational risks and possible oversight limitations for the CSP. In this regard, the assessment should consider certain issues in relation to the aforementioned risks, such as: the selected cloud service; migration and/or implementation processes; the sensitivity of the function and security measures required; the interoperability of the systems of the firm and the CSP, and the portability of data from the firm to the CSP. Lastly, the political stability, security situation and legal system (including the legal regime for insolvencies applicable to the CSP as well as the data protection regime) of the countries where the data would be stored and the functions would be outsourced should be taken into account.
When critical functions are outsourced, the due diligence should include an evaluation of the suitability of the CSP to ensure that it has the business reputation, the skills, the resources (human, IT and financial), the organisational structure and, if applicable, the regulatory authorisation(s) or registration(s) to perform the critical function. Considerations on the following additional factors may be included: information security management, service support, and business continuity plans.

This framework will apply when signing new agreements or upon renewing an existing agreement with a CSP of it is determined that a new due diligence assessment is necessary.

In the responses to the CP, respondents agreed broadly with the approach proposed by ESMA, although many considered that firms should not be requested to provide such an exhaustive assessment of the CSP, including monitoring concentration risk at sector level. ESMA considers that the guidelines provide the appropriate level of guidance in this regard and specifies that firms be mindful of the dominant position of certain CSPs as these providers may not be easily substitutable.

Guideline 3. Key contractual elements

Guideline 3 states that the respective rights and obligations of a firm and of its CSP should be clearly allocated and set out in a written agreement that allows the possibility for the firm to terminate it where necessary. In the case of outsourcing of critical functions, the written agreement must include at least the following: a clear description of the outsourced function; significant dates and notice periods; the governing law; the financial obligations of both parties; whether sub-outsourcing is permitted and if so under what conditions; the location(s) of the outsourced function (including where the data will be processed and stored); information security and protection of personal data; the right for the firm to monitor the CSP's performance; agreed service levels (quantitative and qualitative performance); provisions related to incident management; insurance coverage of certain risks; business continuity and disaster recovery plans of the CSP and, lastly, access and audit rights in respect of the relevant information, facilities, systems and devices of the CSP to the extent necessary to monitor the CSP's performance.Responses to the CP point out that CSPs normally offer standardised contracts that make negotiating contractual terms difficult. They also show concern about the issue of the location of the data and warn of possible overlaps with the GDPR[5]. Some respondents recommend that ESMA, together with EBA and EIOPA, develop standard contractual clauses, which could be adopted by providers and firms on a voluntary basis. ESMA considers that this guideline is an instrument intended to help firms negotiate contractual terms with the CSPs. Likewise, it reiterates the importance of including in the contract a provision regarding the location of the data. Lastly, ESMA agrees with the view that standard contractual clauses may prove beneficial and looks forward to the work that the Commission has undertaken on the topic[6].

Guideline 4. Information security

Guideline 4 states that a firm should set information security requirements in its internal policies and procedures and within the cloud outsourcing written agreement and monitor compliance with these requirements on an ongoing basis. However, it once again specifies that these requirements should be proportionate to the nature, scale and complexity of the outsourced function as well as the risks that may arise from it.In this regard, when the function is considered critical, the requirements will include, at least, the following issues: information security organisation; identity and access management; encryption and key management; operations and network security; application programming interfaces (API); business continuity and disaster recovery; data location and, finally, compliance and monitoring of information security standards and controls.

The opinions given in the responses to the CP indicate that the wording is too prescriptive and does not reflect the different types of cloud outsourcing models; an approach based more on principles is suggested. Lastly, greater alignment with other initiatives is also requested (the Cybersecurity Directive[7], the GDPR and the EBA Guidelines on Outsourcing Arrangements). ESMA believes that the approach is balanced and that the wording takes account of the standards provided in other analogous documents. However, it states that the examples provided are not intended to be exhaustive and it again invokes the principle of proportionality when setting the requirements.

Guideline 5. Exit strategies

Guideline 5 provides that firms must ensure that they are able to exit cloud outsourcing arrangements without disruption to their services, without breaching their legal obligations and without detriment to the confidentiality, integrity and availability of their data. To this end, a firm must develop appropriate exit plans, identify alternative solutions and develop transition plans, and formally secure the support of the outgoing CSP for an orderly transfer.In this regard, it is specified that when developing exit plans, firms should define the objectives of the exit strategy and the triggering events that would activate it. Likewise, they are expected to carry out an impact analysis according to the outsourced function to identify what resources would be needed and assign roles and responsibilities to manage the exit strategy. Lastly, the appropriateness of the exit strategy should be tested, using a risk-based approach. This was a much commented aspect of the CP.

Respondents agreed on the need for a clearly defined exit strategy to avoid disruption of services or detriment to compliance with obligations. However, several questioned the practicality of the exit strategy tests and the requirement for firms to have fully implemented exit plans. Regarding the transfer and/or removal of data, respondents highlighted that the firm, and not the CSP, should be in control of it. ESMA has included comments on the exit strategy tests in its final document. Likewise, provisions related to support for the

orderly transfer are incorporated, along with matters relating to data processing and removal.

Guideline 6. Access and audit rights

Guideline 6 establishes that the contract signed with the CSP should not limit the exercise of access and audit rights by the firm and the competent authorities (or the possibility of their oversight). In addition, the firm must guarantee the effective exercise of these rights in the event of outsourcing a critical or important function. In this regard, it is envisaged that in order to use audit resources more efficiently, and thus reduce the burden, third-party certifications and external or internal audit reports from the CSP may be used. In addition, shared audits may be carried out jointly with other clients of the same CSP, and these may be carried out by a third party appointed by them.The comments received in response to the CP were mainly related firstly to the lack of bargaining power necessary to impose broad access rights on the CSP (for example, on-site inspections are normally restricted) and secondly to practical questions about the use of third-party audit reports and certifications. In response, ESMA once again calls for proportionality and stresses the importance of this issue for proper risk management.

Guideline 7. Sub-outsourcing

Guideline 7 establishes that, in the case of outsourcing to third parties of critical functions already outsourced, the initial written outsourcing agreement between the firm and the CSP must specify any part or aspect of the outsourced function that is excluded from potential sub-outsourcing. In any case, if such sub-outsourcing is permitted, the written agreement between the firm and the CSP must include indications of the conditions to be met and specify that the CSP remains accountable and is obliged to oversee any sub-outsourced services to ensure that all contractual obligations between the CSP and the firms are continuously met; and to notify the firm of any intended sub-outsourcing or material changes thereof. Lastly, the agreement between the firm and the CSP must ensure that the firm has the contractual right to terminate the cloud outsourcing arrangement with the CSP if it objects to the proposed sub-outsourcing or material changes thereof and in case of undue sub-outsourcing.

The issues raised by this guideline elicited multiple comments in response to the initial CP, some of which considered the requirements disproportionate and challenging in certain respects such as delimitation, accountability and notification. Specifically, questions were raised as to whether the guideline was intended to capture the sub-outsourcing of non-material parts of critical functions and about the firms' ability to ensure that their CSPs effectively monitor sub-outsourced functions. In response, ESMA has clarified these issues raised in its final version, although it continues to emphasise the inescapable responsibility of CSPs and firms in these situations. Likewise, it highlights the importance of CSPs' obligation to notify firms of any planned sub-outsourcing and the right of firms to object as important safeguards.

Guideline 8. Written notification to competent authorities

Guideline 8 specifies that the firm must notify its competent authority in writing in a timely manner of planned cloud outsourcing agreements that concern a critical function and of any such arrangements concerning a function previously classified as non-critical that has since become critical. The notification must include, taking into account the principle of proportionality, at least the information defined in Guideline 1 referring to the content of the firm's register of outsourcing arrangements and accompanied by a brief summary of the reasons why the outsourced function is considered critical.The responses received to the CP indicated the need for clarification on the notification process and highlighted some overlaps with other existing notification provisions at the sectoral level. In reply, ESMA believes that the wording of this guideline is sufficiently precise, although it has modified its initial wording to be consistent with Guideline 1. Regarding possible overlaps, ESMA states that the guidelines must be assumed without prejudice to the requirements, guidelines or practices applicable to certain sectors (such as credit rating agencies), which, because they are stricter, could already implicitly meet them[8].

Guideline 9. Supervision of cloud outsourcing arrangements

Guideline 9 specifies that competent authorities should assess the risks arising from firms' cloud outsourcing

arrangements, particularly in relation to critical or important functions. Special attention will be given to outsourced functions performed outside the European Union and, in general, when concentration risks are identified that require special monitoring of the possible impact on the sector and, in general, on the stability of the financial market.

Competent authorities should assess, using a risk-based approach, whether firms have the governance, resources, and operational processes necessary to appropriately and effectively enter into, implement, and monitor their agreements with CSPs. Using the same approach, they will need to identify and manage all relevant risks related to such outsourcing.The responses to the CP show agreement with the proposed approach. Indeed, measures such as this one that promote greater supervisory convergence are appreciated, and any information on concentration risks that can be provided by the competent authorities is considered valuable. ESMA takes note of the responses and refers to the fact that within the framework of DORA it will be possible to further explore concentration risk reporting and harmonisation.

To conclude, ESMA has stated that, among the benefits linked to the introduction of the guidelines, they will support firms in their transition processes to the cloud, providing a consistent framework across sectors, as well as having a limited overall impact in terms of implementation costs. Likewise, it considers that their implementation will reduce the risks of regulatory arbitrage through greater regulatory and supervisory convergence. In other words, the adoption of these guidelines further reduces the risk of divergent interpretations that could lead to discrepancies in the application and supervision of the relevant provisions in the Member States. Lastly, ESMA notes that it has endeavoured to ensure consistency with the EBA and EIOPA guidelines.

[1] EBA/GL/2019/02 – European Banking Authority Guidelines on outsourcing arrangements

[2] EIOPA-BoS-20-002 – European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers

[3] COM (2020) 595 final – 2020/0266 (COD) Proposal for a Regulation on digital operational resilience for the financial sector

[4] CR01/2020 – IOSCO Principles on Outsourcing Consultation Report

[5] 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

[6] Cloud Service Providers consultation meeting on standard contractual clauses for cloud use by financial institutions and Consultation meeting for Financial Institutions on standard contractual clauses for cloud use in the financial sector

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[8] For example, Item 36 of ESMA's Guidelines on Periodic Information Submitted by Credit Rating Agencies

---

Useful links:

- Guidelines on Outsourcing to Cloud Service Providers
- Consultation Document on the Draft Guidelines on Outsourcing to Cloud Service Providers