|  |
| --- |
| Response Form to the Consultation Paper |
| Guidelines on Outsourcing to Cloud Service Providers |

**Responding to this paper**

ESMA invites comments on all matters in this consultation paper on guidelines on outsourcing to cloud service providers and in particular on the specific questions summarised in Appendix I. Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **01 September 2020.**

All contributions should be submitted online at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading ‘Your input - Consultations’.

**Instructions**

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Please do not remove tags of the type <ESMA\_QUESTION\_COGL\_1>. Your response to each question has to be framed by the two tags corresponding to the question.
3. If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.
4. When you have drafted your response, name your response form according to the following convention: ESMA\_COGL\_nameofrespondent\_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA\_COGL\_ABCD\_RESPONSEFORM.
5. Upload the form containing your responses, in Word format, to ESMA’s website ([www.esma.europa.eu](http://www.esma.europa.eu) under the heading “Your input – Open consultations” 🡪 “Consultation on Outsourcing to Cloud Service Providers”).

**Publication of responses**

All contributions received will be published following the close of the consultation, unless you request otherwise. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

**Data protection**

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/legal-notice).

**Who should read this paper**

This paper is primarily of interest to national competent authorities and financial market participants. In particular, this paper is of interest to alternative investment fund managers, depositaries of alternative investment funds, undertakings for collective investment in transferable securities (UCITS) management companies, depositaries of UCITS, central counterparties, trade repositories, investment firms and credit institutions which carry out investment services and activities, data reporting services providers, market operators of trading venues, central securities depositories, credit rating agencies, securitisation repositories and administrators of benchmarks (“firms”), which use cloud services provided by third parties. This paper is also important for cloud service providers, because the draft guidelines seek to ensure that the risks that may arise for firms from the use of cloud services are properly addressed.

**General information about respondent**

|  |  |
| --- | --- |
| Name of the company / organisation | The World Federation of Exchanges |
| Activity | Regulated markets/Exchanges/Trading Systems |
| Are you representing an association? |  |
| Country/Region | Other |

**Introduction**

***Please make your introductory comments below, if any***

<ESMA\_COMMENT\_COGL\_1>

Introduction

We are grateful for the opportunity to respond to ESMA’s consultation regarding its Draft Guidelines on outsourcing to cloud service providers (CSPs).

The World Federation of Exchanges (WFE) is the global trade association for regulated exchanges and clearing houses. We represent over 200 market infrastructures, spread across the Asia-Pacific region (~37%), EMEA (~43%) and the Americas (~20%), with everything from local entities in emerging markets to groups based in major financial centres. Collectively, member exchanges trade some $95 trillion a year; while the 50 distinct CCP clearing services (both vertically integrated and stand-alone) collectively ensure that traders put up $1 trillion of resources to back their risk positions.

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair and transparent environment for all sorts of investors and companies wishing to invest, raise capital and manage financial risk.

We seek outcomes that maximise financial stability, consumer confidence and economic growth. We also engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system.

In the face of the challenging considerations arising from the pandemic in the operation of critical market infrastructure, exchanges and CCPs promptly triggered continuity plans (involving, for example, remote working) to strengthen their operational resilience, against the backdrop of the social-distancing policies that governments around the world adopted.

Market infrastructures recognise their responsibilities as critical elements of the financial system, supplying finance to real economy firms and providing a platform for investors even in times of market stress. Accordingly, they have developed business continuity plans, which in recent months have been executed as necessary. In doing so, market infrastructure businesses have been managing record volumes of trading.

In line with its membership criteria and its members’ own desires, the WFE has long supported the need for market infrastructure to be prepared and as resilient as possible in the face of a wide range of contingencies. For that reason, in previous years the WFE has created working groups, consisting of exchange and CCP experts from across the globe, focused on enterprise and operational risk, as well as on cybersecurity. Operational resilience has been – and continues to be – a priority issue for our membership, and one in which significant time, effort and money has been invested. We therefore welcome the opportunity to offer our perspectives and further contribute to the dialogue, on issues such as outsourcing, in order to secure the shared objectives of fair and orderly markets that promote the safety and resilience of the financial system.

Overview

The World Federation of Exchanges broadly welcomes the proposals and recognises the value of increasing the focus on the resilience of financial services and its third-party service providers, especially in light of the pandemic and its consequences. Technology, and particularly the use of cloud services, plays an ever-increasing role in both professional and domestic lives. The pandemic has further increased the importance of cloud services as workforces operate remotely en masse. Ensuring the continued functioning of that infrastructure is a key objective of market infrastructure firms. The WFE’s members are working closely with CSPs to enhance their resilience and further protect their IT infrastructure with the use of cloud technologies. To that end, the WFE membership recognise – and have implemented measures aimed at addressing – the importance of ensuring the right controls and safeguards are in place around not only critical outsourcing but all forms of outsourcing. The Draft Guidance is helpful in clarifying those expectations and is welcome in its broad application, as the levelling-up of standards across the whole ecosystem of financial services’ operations (e.g. asset managers, banks etc) is vital in achieving operational resilience objectives.

The application of the Draft Guidance to third-country CCPs including Tier 2 third-country CCPs (i.e., those deemed systemically significant to the EU) that comply with the relevant EMIR requirements is also of concern to the WFE membership. The WFE notes paragraph 15 in section 3.1 *‘Scope,’* and would support ESMA adopting an outcomes-based approach to Tier 2 third country CCPs, which adheres to the scope of EMIR 2.2 and the core regulatory principle of international coherence while also seeking to avoid harmful regulatory arbitrage. It is the WFE’s understanding that a policy of mutual deference, which is central to well-functioning cross-border regulatory regimes, would be maintained for Tier 1 CCPs deemed non-systemic.

ESMA’s proposals for Tier 2 CCPs should remain consistent with the authority granted to the home-country regulator of the FMI, which must be able to adopt and apply appropriate regulations that take into account the home-country legal regime, market structure and trading practices. Different jurisdictions will naturally have different requirements, but that does not necessarily mean those requirements deviate from internationally agreed standards. The rationale for the Principles for Financial Market Infrastructures (PFMI),[[1]](#footnote-2) which set out globally agreed standards for FMI risk management, is to allow policy makers to tailor their regulatory frameworks to the specific characteristics of their markets while respecting international norms.

In this regard, the WFE would also recommend the linking or indexing of related international standards which relate to control frameworks, e.g., ISO standards (27017), as they would be beneficial in ensuring a common understanding and implementation of the Guidelines.

<ESMA\_COMMENT\_COGL\_1>

**Questions**

1. : Do you agree with the suggested approach regarding a firm’s governance and oversight in relation to its cloud outsourcing arrangements? Please explain.

<ESMA\_QUESTION\_COGL\_1>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_1>

1. : Do you agree with the suggested documentation requirements? Please explain.

<ESMA\_QUESTION\_COGL\_2>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_2>

1. : Do you agree with the suggested approach regarding the pre-outsourcing analysis and due diligence to be undertaken by a firm on its CSP? Please explain.

<ESMA\_QUESTION\_COGL\_3>

* **Section 3.5, Guideline 2: 33.a) (vii). Possible concentration within the firm**. While it is reasonable and desirable for a firm or group to consider its *own* degree of concentration vis-à-vis a given CSP, it is not clear how in practical terms such a firm/group could ascertain how many of its peers are also using that same CSP. CSPs are typically restricted by contract from disclosure of other firms’ use of the services. The drafting might therefore benefit from being rephrased to focus on the user-firm’s ‘knowledge and recommended evaluation of risk’. There is also potential for a disproportionate approach, as compared with policy on the use of technology more generally. Additionally, use of a given CSP by more than one firm does not affect the resilience of that CSP’s cloud operations.

<ESMA\_QUESTION\_COGL\_3>

1. : Do you agree with the proposed contractual requirements? Please explain.

<ESMA\_QUESTION\_COGL\_4>

* **Section 3.5, Guideline 3: 39**. As it stands, this article could place an undue administrative burden on market infrastructure and does not address the point raised previously in the Proposed Guidelines that the consideration of a CSP’s obligations and offering is not limited to the terms of the contract. As noted previously in the Proposed Guidelines, the regulated entity is ultimately responsible for compliance. In addition, many requirements – particularly technical, operational, and functional requirements – are not addressed in the terms of the contract, but in the CSP’s policies and procedures, third-party audits, certifications, and governance practices. Thus, a regulated entity must consider and address the elements of CSP outsourcing not only by way of the contract with the CSP, but also through a review of those policies, and procedures, third-party audits, etc. For example, a firm may decide not to outsource certain services related to records management or encryption key management. In these situations, the written legal agreement would not address those functions, though it would remain the firm’s responsibility to explain its arrangements to competent authorities.
* **Section 3.5, Guideline 3: 41**. We propose the revision to the opening sentence, “In case of outsourcing of critical or important functions, ~~the written agreement should set out at least:~~ *the following topics should be addressed in the written agreement or, where appropriate, detailed in writing in the CSP’s policies and procedures, third-party audits, certifications or governance practices*:” The items listed in this subsection are of importance but, as discussed above, may be addressed outside of the contract with the CSP, or obligations retained by a firm (e.g., records management) should appear instead in its internal policies and procedures.
* **Section 3.5, Guideline 3: 41(n).** Proposed revision, “the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by ~~the firm or the competent authorities the right to access (‘access rights’) and to inspect (‘audit rights’) the books, premises, relevant systems and devices of the CSP to the extent necessary to monitor the CSP’s performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements, having regard to Guideline 6~~; *these groups the right to access and inspect the CSP, having regard to the application of both Guidelines 6 and a risk-based approach*.” In practice CSPs may be reluctant to grant access and audit rights to books and premises. As noted in Guidelines 6, other approaches, such as certifications or group audits, may satisfy these requirements.

<ESMA\_QUESTION\_COGL\_4>

1. : Do you agree with the suggested approach regarding information security? Please explain.

<ESMA\_QUESTION\_COGL\_5>

* **Section 3.5, Guideline 4: 42.** We propose the following revision – “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, including to protect confidential, personal or otherwise sensitive data. *Additionally, the CSP written agreement may also include a requirement to have a written information security programme, having regard to the application of the applicable elements of Guideline 4.*” The CSP written information security programme, along with the negotiated language of the legal agreement, permits firms to appropriately address information security outsourcing risks.
* **Section 3.5, Guideline 4: 43.** We propose that all instances of “ensure” (suggesting a prescriptive requirement) are modified to “*evaluate, assess, or consider*” (suggesting a best practice). Whilst the inclusion of prescriptive requirements does not appear to be the intent, rather the goal should be to provide a roadmap for topics to consider following a risk-based approach in this context. This change would help clarify that proposal.

<ESMA\_QUESTION\_COGL\_5>

1. : Do you agree with the suggested approach regarding exit strategies? Please explain.

<ESMA\_QUESTION\_COGL\_6>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_6>

1. : Do you agree with the suggested approach regarding access and audit rights? Please explain.

<ESMA\_QUESTION\_COGL\_7>

* **Section 3.5, Guideline 6: 47.** Proposed revision~~, “A firm should ensure that the cloud outsourcing written agreement does not limit the firm’s~~ *A cloud outsourcing written agreement should not inappropriately limit a* firm’s effective exercise of access and audit rights or its oversight options on the CSP, *including those mentioned in* *Section 3.5, Guideline 6: 50*.” The proposed change reflects a risk-based approach (“not inappropriately limit”) and references to other sections of the Proposed Guidelines.

<ESMA\_QUESTION\_COGL\_7>

1. : Do you agree with the suggested approach regarding sub-outsourcing? Please explain.

<ESMA\_QUESTION\_COGL\_8>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_8>

1. : Do you agree with the suggested notification requirements to competent authorities? Please explain.

<ESMA\_QUESTION\_COGL\_9>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_9>

1. : Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain.

<ESMA\_QUESTION\_COGL\_10>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_10>

1. : Do you have any further comment or suggestion on the draft guidelines? Please explain.

<ESMA\_QUESTION\_COGL\_11>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_11>

1. : What level of resources (financial and other) would be required to implement and comply with the guidelines and for which related cost (please distinguish between one off and ongoing costs)? When responding to this question, please provide information on the size, internal set-up and the nature, scale and complexity of the activities of your organization, where relevant.

<ESMA\_QUESTION\_COGL\_12>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_12>

1. Published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO); *available at* <https://www.bis.org/cpmi/info_pfmi.htm>. [↑](#footnote-ref-2)