|  |
| --- |
| 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 | Depository Trust & Clearing Corporation (DTCC) |
| Activity | Other Financial service providers |
| Are you representing an association? |  |
| Country/Region | North-America |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

The Depository Trust and Clearing Corporation (“DTCC”) welcomes the opportunity to respond to the European Securities and Markets Authority (“ESMA”) Consultative Document, “Draft Guidelines on Outsourcing to Cloud Service Providers” (“Consultation”)[[1]](#footnote-2).

DTCC provides a wide range of post-trade services across the financial services industry, including trade repositories that provide global compliance reporting for derivatives transactions across all asset classes, among them our Europe-based DTCC Derivatives Repository Ltd. (DDRL) and DTCC Data Repository (Ireland) Plc (DDRIE). DTCC also offers clearing and settlement and asset servicing for the majority of equity and fixed income trading in the U.S., services to support the wealth management and insurance industries, institutional matching and post-trade management services.

DTCC appreciates that ESMA has considered the European Banking Authority (EBA) Guidelines on Outsourcing Arrangements[[2]](#footnote-3) in the development of this Consultation as this creates a consistent cloud outsourcing regulatory framework across the European Economic Area and reduces the probability of regulatory fragmentation.

Where there is appropriate internal governance, processes and oversight, cloud services can offer numerous potential benefits over on-premises technology, including improvements in resilience, scalability, cost-efficiency, automation, flexibility and security. As a result, many financial institution business functions use public cloud-based services. Risk areas continue to exist, however, as outlined in the Consultation[[3]](#footnote-4). We believe the Consultation provides an important step towards helping financial institutions identify, monitor and address risks that may arise from their cloud outsourcing arrangements. Given the importance of this work to our business and our markets, we offer the following comments for your consideration.

General Comments

DTCC agrees that the risk areas identified in the Consultation are important areas that financial firms should consider when deciding to move services to a cloud-based environment. More specifically, DTCC agrees that financial institutions should:

1. Have appropriate governance and oversight of cloud service providers (CSPs) including senior management engagement and oversight;

2. Execute specific due diligence activities prior to contract signing to understand business and IT risks to the new technology delivery model;

3. Monitor their CSPs to identify service degradation or increased security risks;

4. Identify new information security risks based on threat landscape and evolving business operations;

5. Have documented and tested exit strategies for critical or important business services; and

6. Understand the legal/regulatory implications of having data located in a country inside or external to the EEA (e.g., authority access to data; regulator access to data in the event a financial institution becomes insolvent)

However, DTCC notes that challenges may exist between financial institutions and CSPs regarding execution of certain requirements identified in this Consultation. The following are thematic challenges that will be further outlined in detailed examples in response to the Consultation questions.

Third Party Contractual Relationships

Financial institutions and CSPs range from small institutions and service providers to large institutions and technology providers. The contractual relationships between these two entities vary widely from procuring commodity infrastructure and IT components to the engagement of strategic outsourcing of critical business systems and systems that store confidential data (e.g., personally identifiable information). In general, a financial institution’s risk assessment model factors the potential business impacts of these relationships to determine the criteria for governance. However, the size of the financial institution may have a significant impact on the effectiveness of third-party risk management. When negotiating with large CSPs, large financial institutions may have significant power in negotiations and may stipulate ongoing assessments due to the amount of revenue at stake. Smaller institutions may not have the same leverage and therefore may be held to standard contractual terms for the vendor service. Nonetheless, these smaller financial institutions may receive greater security and resilience advantages through their use of cloud services when compared to large financial institutions, in part, because CSPs provide them with greater access to highly skilled cyber and IT resources than they would otherwise have.

In addition, a financial institution’s policies and standards will vary widely based on the size, type and complexity of its business operations, its customers and counterparties, the markets in which it operates, and the products traded on those markets; and market interconnectedness. These policies and standards further inform contractual requirements with vendors. CSPs and financial institutions take care in their contracts and other arrangements to address the challenge associated with meeting each financial institution’s unique information security requirements. Given these variances between financial institutions, CSPs could be required by contract to adhere to scores of different security and monitoring requirements with differing frameworks for managing risks, which may not be necessary depending on the facts and circumstances of the arrangement between the parties.

Financial institutions are held to high regulatory standards, and those standards have been built and enforced in current on-prem infrastructures. CSPs that do not, or cannot, support those standards simply cannot be used.

Thus, policy makers should avoid prescriptive and granular requirements in this regard.

DTCC agrees that outlining security requirements as well as the roles and responsibilities of both the CSP and financial institution are necessary to deliver a secure environment for business operations. It further recommends that regulatory requirements around the level of detail contained in these information security provisions be more principles-based to provide needed flexibility to financial institutions and CSPs to address changing threat landscapes and bespoke needs.

Concentration Risks

As the market structure continues to evolve through the influx of new market entrants and the use of new and emerging technology, financial institutions have reviewed their operations to identify opportunities to lower operational costs and increase profit margins[[4]](#footnote-5). Commodity cloud services have provided financial institutions with the opportunity to maximize IT capital expenditures through a flexible and scalable environment, while maintaining and, in some cases, increasing the level of security and resilience in the financial services sector. Although these benefits are being realized by the financial services sector, the selection of CSPs that are able to accommodate and achieve the safety and soundness requirements of the financial services sector is limited and may also impact potential exit strategies for financial institutions that need to transfer services in the event of a material operational incident.

Understanding the concentration risks across the financial services sector, while important, may not be achievable by individual financial institutions due to lack of visibility of CSPs usage outside of its organization. Financial institutions would need to rely on both the supervisors and international standards setters to understand these risks and associated market impacts. DTCC requests that the authorities consider providing these insights back to financial institutions in a manner that allows institutions to integrate this risk into their risk management facilities.

Exit Strategies

The ability to exit/terminate vendor provided services has been part of numerous supervisory requirements[[5]](#footnote-6). Financial institutions have and continue to work with CSPs to develop new and innovative ways to build security and resilience into the CSP service offerings. However, there are two trends that may impede the ability of financial institutions to transfer services in a manner that results in undue disruption to its business activities and services. First, there is a consolidation in many enterprise software SaaS solutions which may limit a financial institution’s selection to one or two providers. Second, a primary benefit for financial institutions using CSP services is the use of the CSP tools and code libraries that maximize the cloud experience and consistently develop business applications on a common framework. This benefit may result in the limitation of a financial institution to exit or transition a service to another CSP in an emergency situation (i.e., unplanned exit). Additionally, as financial institutions move to CSP environments, they decrease their data center footprint. The combined lack of data center capacity and access to code libraries may limit or make obsolete the ability to transition services in house.

Given these trends, DTCC recommends that ESMA consider working with the financial services sector prior to drafting specific, prescriptive rules in this area. Additional engagement will allow supervisors and financial institutions to identify viable solutions that address these trends as they relate to requirements around exit strategies in an equitable manner that allows financial institutions to avail themselves of the benefits associated with Cloud adoption.

ESMA Consultation Comments

The Consultation outlines potential requirements in nine risk areas. Where possible, DTCC’s comments focus on the challenges and potential amendments to further bolster the expressed objectives.

<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>

DTCC agrees with the suggested approach [and has aligned its governance and oversight in a way that aligns to the rules set forth in this section]. DTCC also agrees with the need to have an inventory of vendors, including CSPs, and recognizes that the data elements listed are aligned to those required by the EBA Guidelines on Outsourcing. However, DTCC believes that these data elements may not be necessary to gain an understanding of the importance of the CSP to the institution’s business operations or to singularly identify a CSP service in use by the institution. For example, DTCC determines the CSP criticality by the hosted application’s business continuity requirements and regulated data content (e.g., personally identifiable information) together with the criticality of the business functions. While this approach results in the same outcome, the format is different than what is outlined in Paragraph 29c – 29e. In addition, it is common for the application-to-CSP relationships to be documented in a technology database while application-to-function relationships are documented in a process modeling or business continuity database. Therefore, DTCC requests additional clarity from ESMA on whether this information may be obtained by various sources versus a singular database.

<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>

DTCC agrees with the provisions set forth in this section and supports the use of standards-based certifications to validate that the cloud services control environment is adequate and effective. There are certain provisions however, that could present implementation challenges for the financial services sector. Many financial institutions take advantage of a CSP’s code libraries and other cloud service features to gain full access to the benefits of cloud services and to create a more uniform application environment. This usage and uniformity allow financial institutions to better secure their environment through standardization. It also allows them to foster more efficient cybersecurity mitigation strategies (e.g., application penetration testing, vulnerability management). DTCC notes that while there are clear security and resilience benefits for using these libraries, they also create the potential for vendor lock-in. These libraries are often vendor-specific and may not exist at other viable, cloud service providers, which limits the ability to easily port the service in a stressed (unplanned) exit of the CSP service. However, this concern should be balanced against the fact that since CSPs have varying strengths and capabilities, once an institution starts extrapolating functionality across cloud vendors, many of the benefits get lost as the CSP’s capabilities are neutered. Rather than setting forth prescriptive portability requirements, DTCC recommends a flexible principles-based approach that allows institutions to mitigate Cloud use risks in a manner that aligns with the firm’s resilience strategy. For example, an institution might choose to port highly sensitive data back on prem in lieu of moving to a different CSP.

In addition, section 33a(vii) stipulates that financial institutions should understand ‘the possible concentration risks within the Sector caused by multiple firms making use of the same CSP or a small group of CSPs.’ Financial institutions are unable to make this assessment because they do not have the visibility into CSP usage by other institutions. Even where such information might be known, financial institutions may not understand the true concentration risks associated with use of a CSP or a small group of CSPs because they will likely be unable to fully appreciate the use of cloud services by other third parties (i.e., fourth party service providers) or the types of services and functions other parties are placing into the cloud. The financial services sector would need to rely on regulatory authorities to understand the broader concentration risks and associated market impacts. Further, the marketplace for cloud services continues to trend toward a small number of viable CSP options that meet the criteria set forth in the Consultation[[6]](#footnote-7).

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

Contract negotiations set the stage for financial institutions and CSPs to explicitly state the obligations of each party for the course of the agreement. However, depending on their size and associated bargaining power, financial institutions may be limited in their ability to negotiate contract terms. More specific to this Consultation, the terms set forth in paragraphs 41c, 41j, 41l, 41m and 41n are not standard contractual terms. Where small and medium-sized institutions do not have the negotiating power necessary to include these provisions in their agreements, they will not be able to comply with these requirements. Similarly, paragraphs 41j and 41n are difficult, if not impossible, provisions for all financial institutions to negotiate into a contract. For 41j, while financial institutions may be able to gain access to third party reports (e.g., SOC2), access to a CSP’s internal audit reports are not part of a CSPs standard contract language and may be difficult for small/medium financial institutions to negotiate into its contracts. For 41n, the ability for financial institutions to gain access to a CSPs books and records may also be difficult to negotiate into a CSPs standard contractual agreements.

Further, right to audit clauses, especially the books and records of large CSPs, have proven challenging for financial institutions of all sizes.

CSPs have multiple data centers which may contain a portion of a financial institution’s data. The physical access controls implemented at each of these data centers may differ by region, country, or vicinity of the data center location.

Contractual terms with the CSP could include the ability of the supervisor to have an onsite visit, however, this may be of limited value given the geographic dispersion of an institution’s data.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

DTCC agrees with most of the provisions outlined in this section. Financial institutions should establish information security requirements and define the roles and responsibilities in the contractual service terms. Additionally, financial institutions should have the capability to monitor and otherwise have oversight of the CSP to gain assurance that the contractual terms are met. However, there are some provisions that may present implementation and compliance challenges.

Paragraph 43e reads that a firm should ‘consider mechanisms for the integration of the cloud services with the systems of the firm to ensure security of APIs.’ While this is a good security practice, a financial institution may increase its reliance on the CSP to provide application services and increase the time needed to exit the CSP in the event of an unplanned exit.

In addition, paragraph 43f suggests that financial institutions may have the ability to request and review CSP documentation showing the transport route of its data. Gaining this level of access to a CSP’s network infrastructure details may prove challenging and create unnecessary cybersecurity risks. Just as financial institutions would consider this information to be confidential and non-receivable to its clients, CSPs may take a similar position regarding allowing multiple financial institutions access to, and retention of, this data. Moreover, it is unclear what access to this information would provide a financial institution from a resilience perspective.

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

Exit strategies play a critical role in providing a level of assurance that financial institutions are prepared for severe third-party operational outages. Testing these exit strategy serves to decrease the operational friction that may occur during a real event. DTCC believes that any strategy that is employed by financial institutions should (1) balance the distribution of risk management between the financial institution and CSP and (2) foster a safe and reliable functioning of the financial markets.

The Consultation notes that ‘a firm should develop exit plans that are comprehensive, documented and sufficiently tested.’ This language suggests that financial institutions and CSPs be required to perform systems testing to provide a certain level of assurance that a financial institution’s service may be transitioned to another CSP. Such a requirement could result in a many-to-one testing regime where the CSPs are required to conduct hundreds of burdensome and costly tests for each financial institution client to allow financial institutions to meet their compliance obligations. Second, CSPs are not the sole critical infrastructure within the financial services sector. This testing regime could potentially be extrapolated to other critical market infrastructure (e.g., clearing, settlement, payments) where the ability to conduct this volume of additional tests is extremely limited based on available cyber expertise, market costs, infrastructure capacity, and security concerns. Third, the ability to conduct a full exit strategy test would require financial institutions to have a fixed destination to test the service transition. An exit strategy is dependent on the final destination of the data, application, or service and a full testing requirement could force financial institutions to maintain two or more cloud environments, which would substantially increase overall costs associated with cloud usage, including but not limited to internal testing costs, thereby mitigating any potential costs savings associated with using cloud services. For example, financial institutions would not only be required to test with CSPs, they would also need to continuously test the portability of applications and services upon its own application changes or changes to the CSPs service offerings to provide assurance that these services can be transferred without undue delay or impact to business services.

In addition, DTCC believes ESMA should differentiate between planned exits and stressed or unplanned exits under this Guideline. The use of planned exits between financial institutions and CSPs allow financial institutions and CSPs to execute phased transitions to new computing environments. On the other hand, stressed or unplanned exits due, for example, to a material service outage may limit a financial institution’s ability to seamlessly transition the service or allow the CSP to assist with the transition of the service[[7]](#footnote-8). An exit strategy should incorporate elements of both planned and stressed scenarios to avoid the development of two separate exit strategies so that requirements under this guideline are appropriately applied if and as necessary under each scenario[[8]](#footnote-9). Clarity in this regard would further serve to align a financial institution’s compliance practices with supervisory expectations.

Finally, as noted in our General Comments, there is a limited number of viable CSPs. The ability to port applications from one CSP to another or back in-house requires a significant investment of time and money from both the financial institution and the CSP. These costs together with the loss of competitive advantage and return on technological investment may disincentivize CSPs from putting forth the necessary effort and impede a financial institution’s ability to transition its applications and services. Similar to other data sharing initiatives (e.g., PSD2), additional initiatives may be required to decrease the operational friction that exists for data porting between CSPs. As a final point, Paragraph 44d requires that ‘a firm should ensure that any data removed or transferred is securely deleted from the systems of the CSP.’ DTCC requests confirmation that secure deletion may also include cryptographic deletion where the data may remain on the CSP’s system but the cryptographic keys to the data are destroyed rendering the content unreadable[[9]](#footnote-10). This method of deletion provides financial institutions with greater control of the removal of data from the CSP environment by rendering it unreadable/unencryptable by either party.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

While DTCC agrees that the provisions in this section may serve to balance the financial institution’s risks, the concentration of cloud services to a handful of viable CSPs that can meet the supervisory requirements combined with the contractual challenges described above under Guideline 3[[10]](#footnote-11) limit the ability of financial institutions to successfully negotiate these terms into contracts.

<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>

DTCC agrees that ESMA should be made aware of a financial institution’s intention to outsource functions that are critical to its business services. This notification should be done in a manner that provides the authority with sufficient time to understand the financial institution’s assessment of the strategic, operational, legal, information security and resilience risks. The ability to conduct this review allows ESMA to understand both the risk to the financial institution and the Sector as a whole. DTCC requests that ESMA clarifies the notification period required by the authority when outsourcing a critical business function so that the financial institution is informed of the larger Sector risks that may not be apparent to the financial institution based on its limited visibility of the Sector’s use of CSPs. DTCC further requests that any time frame needed by the authorities be made clear. This will allow the financial institution to better plan any service transition to the CSP environment.

<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>

In order to understand the concentration risks that may exist across the financial services sector, DTCC requests that competent authorities not only monitor these risks but also report these risks back to the sector to promote greater visibility and understanding of CSP concentration risk.

<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. ESMA, Draft Guidelines on Outsourcing to Cloud Service Providers (06 March 2020), available at <https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf> [↑](#footnote-ref-2)
2. EBA (2019), EBA Guidelines on Outsourcing Arrangements available at <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf> [↑](#footnote-ref-3)
3. Consultation at 6,7 [↑](#footnote-ref-4)
4. FSB (2019), BigTech In Finance, pg 19: <https://www.fsb.org/wp-content/uploads/P091219-1.pdf> [↑](#footnote-ref-5)
5. SIFMA developed a list of outsourcing supervisory requirements where termination required the use of exit strategies. While additional supervisory requirements have been issued since the 2014 publication, it is illustrative of this requirement. SIFMA (2014), Outsourcing Matrix, <https://www.sifma.org/wp-content/uploads/2017/08/summary-third-party-regulation-mapping-table.pdf> [↑](#footnote-ref-6)
6. Consultation at 19, paragraph 34 [↑](#footnote-ref-7)
7. Consultation at Paragraph 44c [↑](#footnote-ref-8)
8. Consultation at Paragraph 45 [↑](#footnote-ref-9)
9. https://en.wikipedia.org/wiki/Crypto-shredding [↑](#footnote-ref-10)
10. Reference the Third Party Contractual Requirements within this document [↑](#footnote-ref-11)