# Financial Institutions' Management of Third-Party Risk and Outsourcing Stocktake: questionnaire for external stakeholders

On 9 November 2020, the Financial Stability Board (FSB) published a discussion paper for public consultation on *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*.[1] The discussion paper invited comments from external stakeholders on: (i) the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships (including risks in sub-contractors and the broader supply chain); (ii) possible ways to address these challenges and mitigate related risks, including in a cross-border context; and (iii) lessons learnt from the COVID-19 crisis relating to outsourcing and third-party relationships.

The public consultation period for the discussion paper ended on 8 January 2021, and 39 responses were received from a wide range of stakeholders including banks, insurers, asset managers, financial market infrastructures (FMIs), third-party service providers, industry associations, individuals and public authorities.[2] In addition, the FSB's Standing Committee on Supervisory and Regulatory Cooperation (SRC) held a virtual outreach meeting on 22 February 2021 to discuss: evolving industry practices; practical challenges associated with outsourcing and third-party risk management; and potential ways to improve coordination among the relevant stakeholders (i.e. supervisory and resolution authorities, financial institutions and third-party service providers) with a view to enhancing the resilience of financial institutions and the financial system.

Based on the dialogue with external stakeholders, the SRC, through its Workstream on Third-Party Risk (hereafter WS), decided to develop: (i) expectations for financial authorities' oversight of financial institutions' reliance on service providers; as well as (ii) common definitions and terminologies on third-party risk management and outsourcing.[3] It is expected that a consultative document to be prepared by Q1 2023. To this end, the WS has started to take stock of practices and challenges in relation

[1] FSB (2020) *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*, 9 November.
[2] See FSB website for individual public responses. For an overview of responses from external stakeholders, see FSB (2021) *Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships: Overview of Responses to the Public Consultation*, 14 June.
[3] See FSB (2022) *FSB Work Programme for 2022*, 31 March and FSB (2022) *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors: February 2022*, 17 February.

to authorities' expectations on financial institutions' third-party risk management and outsourcing.

Since practices for managing third-party risk and outsourcing are evolving rapidly and involve a wide range of external stakeholders, the SRC-WS recognise the importance of obtaining inputs from external stakeholders early in the process where possible and learn from such inputs. Therefore, the SRC-WS has prepared the attached questionnaire for selected external stakeholder experts to share their views on financial institutions' practices and challenges in managing their relationship with third-party service providers that they deemed to be critical (i.e. critical service providers). Specifically, the questionnaire is asking inputs on the following four points:

- Commonly-used terms and definitions in relation to third-party risk management and outsourcing (Section A);
- Framework, process and challenges in managing relationships with critical service providers (Section B);
- Monitoring and managing risks from ongoing critical services provided by critical service providers (Section C); and
- Managing risks and ensuring resilience associated with a disruption of critical service providers (Section D).

External stakeholder experts are kindly asked to **respond to the questionnaire on this FSB online survey tool by Thursday 26 May.** All responses will be shared with the SRC-WS members on a restricted basis (i.e. not for publication and not to be quoted) and used only for the purpose of SRC-WS work. The respondents to the questionnaire will be invited to a workshop organised by the SRC-WS to discuss financial institutions' practices and challenges in managing their relationship with critical service providers, and may be asked to engage with the SRC-WS to provide technical inputs on the topic going forward. In responding to the questionnaire, responding experts are kindly asked to provide views based on his/her experience and understanding of the topic, and not necessarily views of particular industry or firm he/she is affiliated with.

For questions regarding the questionnaire, please contact the FSB Secretariat (email: Yasushi.Shiina@fsb.org and Takao.Miyamoto@fsb.org).

## General information

Jursidiction (country): Germany

Organisation/s: Deutsche Börse AG and its Affiliates (hereinafter collectively "Deutsche Börse Group" or „DBG")

*Contact person 1:*
Name: Tobias Strobel
E-mail address:
Phone number:

*Contact person 2:*
Name:
E-mail address:
Phone number:

## Part A: Commonly-used terms and definitions

1. What are the key terms and definitions used by financial institutions in their third-party risk management and outsourcing including, if applicable, in their group/global third-party risk management programmes?[4]

| |
|---|
| European regulators, but also EU Member State level regulators have already established regulation on outsourcing which includes outsourcing and third-party risk management related definitions (e.g. the EBA and ESMA guidelines on outsourcing).<br>Currently, the European Commission is working on several legislative initiatives including the Digital Operational Resilience Act (DORA), which will introduce a further range of standardized definitions establishing a basis for contracting outsourcing arrangements in the European Union.<br>DBG always seeks to synchronize its contractual language with terms and language introduced by regulation. |

[4] Examples of key terms and definitions may include but not limited to "outsourcing", "third-party risk", "dependency management", "criticality", "importance", and "materiality".

2. Among the terms listed in Q1, are there any terms that you see benefits in establishing a globally consistent definition?

We do see the necessity to establish a globally consistent set of definitions and strongly support the global alignment towards consistent and harmonized definitions, as global operations of enterprises will massively benefit from a common set of terms that are not subjected to internationally diverging interpretation. Such harmonized set of definitions will also contribute to opening up a level playing field for international actors, facilitating international activities. Please see as definitions in DORA, EBA, Guidelines on outsourcing arrangements ESMA Guidelines on outsourcing to cloud service providers.

## Part B: Financial institutions' management of critical service providers

3. How do financial institutions define and identify critical services providers? Do they have processes that differentiate the criticality of different providers? Do they have processes that differentiate the criticality of different services?

There are processes in place to classify services provided by third parties (incl. internal service providers) by their relevancy according to applicable regulations, to identify respective risks and to mitigate them.

4. How do financial institutions identify and map people, processes, technology and third parties involved in delivery of services provided by critical service providers for effective dependency management?

There are processes in place to classify services provided by third parties (incl. internal service providers) by their relevancy according to applicable regulations, to identify respective risks and to mitigate them.

5. What are the main challenges that financial institutions face in managing their relationships with critical service providers?

Main challenges:

- Risk of Vendor lock-in
- No standard contract clauses for basic outsourcing requirements (e.g. as required under EBA/ESMA Guidelines – typical focal point of intensive negotiations
- Long sub-outsourcing chains
- Potential concentration of third-party providers on micro and macroeconomic level.
- Data protection and other ICT related rules differing from jurisdiction to jurisdiction
- Business Continuity Measures

6. How do financial institutions take into account concentration and cross-border aspects of service providers in managing their relationships with critical service providers at the level of individual financial institution's dependence on a service provider? How do financial institutions consider or measure such concentration? What are the main challenges and limitations they face in doing so?

DBG is aware of macroeconomic concentration risks, however these have only low visibility from an individual company perspective as no impartial information on the macroeconomic perspective is available, yet. DBG would appreciate if supervisory authorities would provide information and assessments on the macroeconomic concentration risk to financial industry actors in order to help increase capital markets stability.

DBG identifies and manages its concentration risks and dependence on service providers on the micro level to mitigate concentration risks, i.e. via a multi-cloud strategy.

7. How do financial institutions take into account concentration and cross-border aspects of service providers in managing their relationships with critical service providers at the level of financial sector or system as a whole's dependence on a service provider? How do financial institutions consider or measure such concentration? What are the main challenges and limitations they face in doing so?

Please see Q6

## C. Monitoring & managing risks from ongoing critical services provided by critical service providers

8. How do financial institutions monitor and manage risk from the ongoing critical services provided by critical service providers? Specifically:

(i) What information items do financial institutions request from critical service providers and how frequently?

The type and frequency of reports required from critical service providers diverges from service to service. However, it can be concluded, that DBG requires its critical service providers to provide KPI reports, risk reports and to grant an unconditioned and unrestricted audit right. A further measure is to establish governance structures with critical service providers that foster regular meetings and discussion between the service provider and DBG.

(ii) In general, how able and willing are critical service providers to provide requested information items? What types of information that financial institutions deem necessary are not provided? If any difficulties are experience, what are the reasons behind it?

Different information is needed:

1) Onboarding process related information
2) Supplementary information in the longer run
3) Information on developments that could have adverse effect on the sourced services

DBG also requires unconditional and unrestricted audit rights from its critical suppliers. Dependent on the maturity of critical service provider's organization and their exposure to financial industry requirements we encounter different levels of reluctance to accept DBG to grant audit rights and to accept the obligation to disclose audit reports, including audit reports of the service provider's own internal audit team. Mostly these rights and obligations are subject to resource intensive negotiations.

(iii) How do financial institutions use information obtained from critical service providers?

The received information is thoroughly analyzed and taken into account to establish a comprehensive picture of the circumstances of a potential or actual outsourcing. Based on the analysis mitigating measures are being implemented whenever required and possible. If no mitigation is possible the eligibility of a service provider to provide services will be challenged.

(iv) What kind of organisational and functional approach do financial institutions take in managing their relationship with critical service providers, including the role of the various lines of defence for risk management?

DBG has established a three lines of defense approach in order appropriately manage its risks. Control functions (Compliance, Risk Management, Legal, Outsourcing Management, Business Continuity Management, Information Security and Data Protection) are directly involved in assessment of risk for outsourcings.

(v) What approaches do financial institutions rely on to obtain assurance and information on the critical services from critical service providers? What are the respective benefits and challenges of these approaches? Examples may include but not be limited to: individual audits and on-site visits, use of pooled audits and on-site visits, and commonly (either internationally, regionally or nationally) recognised certifications.

DBG has initiated the Collaborative Cloud Audit Group (CCAG) in 2017 that allows CCAG members from the financial industry to conduct joint audits on cloud service providers. The scale effects of such joint audits leveraged the quality of audits, as larger resources can be deployed in an audit while they reduced efforts of the cloud service provider as the number of individual customer audits is lowered. We see the potential of such joint audits also for other service providers who offer standardized multi -client services to the financial services industry.

## 9. How do financial institutions ensure data transferred to critical service providers for critical services are handled in accordance with contractual specifications?

DBG uses data encryption at rest and in transit, uses service provider supplied information and internal audit reports as well as external audit reports provided by its service providers and audits critical service providers, including audits for data handling and information security (e.g. via penetration testing)

There are two levels of measure in place to protect data transfers.

1. Technical measures:
   All data is encrypted with BYOK “bring your own key”, logs are consolidated in monitored in DBG SIEM to detect any unwanted data access and transfer, lock box services are implemented
1. Organisational measures:
   Data related controls are focus areas for supplier audits to verify that contractual specifications are kept.

## 10. How do financial institutions assess the reliability of critical service providers’ business continuity plans for critical services?

No response

11. In general, how do critical service providers' business continuity plans fit in with their financial institution clients' plans for business continuity?

As it is often not viable for multi-client service providers to provide individual plans for business continuity to the financial institutions, DBG at times when using such multi-client service providers has to adapt to the given circumstances.

12. How do financial institutions test their plans for business continuity in relation to a possible disruption of the critical services provided by their critical service providers?

That depends on the services, e.g. firedrills are a means for CCM testing

13. Do financial institutions conduct joint testing and recovery exercises (e.g. threat led penetration test, scenario exercise, stress test) with their critical service providers? If so, how frequently?

Yes. Penetration testing is a requirement inter alia under the EBA and ESMA outsourcing guidelines.

14. When financial institutions test cyber resilience, what are the challenges faced by financial institutions where critical functions are delivered, either totally or partially, by critical service providers?

One interesting item is that the industry practice of pen testing white hat teams is that vulnerabilities discovered in pen testing are notified to the producer of the item bearing the vulnerability with a lead time to resolve the vulnerability. After that lead time typically the vulnerabilities are published as CVE's to the public. This practice often stands in contradiction to standard confidentiality agreements of the principal with the producer of the vulnerable item.