FSB FINANCIAL STABILITY BOARD

Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

Discussion paper

9 November 2020

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Regulatory and supervisory issues relating to outsourcing and third-party relationships

Background

In December 2019, the Financial Stability Board (FSB) published a report on *Third-party dependencies in cloud services* that explored potential issues for supervisory authorities and financial stability stemming from the scale of services provided via the cloud and the small number of globally dominant players providing such services. Many issues highlighted in the December 2019 FSB report are not just relevant to cloud services but to outsourcing and third-party relationships in general. The report also concluded that further discussion among supervisory and regulatory authorities on current approaches to the management of outsourcing and third-party risks and of relevant regulatory and supervisory approaches would be constructive. In January-March 2020, the FSB Standing Committee on Supervisory and Regulatory Cooperation (SRC) conducted a survey among its member jurisdictions on the existing regulatory and supervisory landscape relating to outsourcing and third-party risk management, including cross-border supervisory challenges and potential financial stability issues (SRC survey).

This Discussion Paper was developed on the basis of this survey. It presents an overview of the current and evolving regulatory and supervisory landscape on outsourcing and third-party risk management in FSB-SRC member jurisdictions. It is intended to facilitate and inform discussions among authorities (including supervisory and resolution authorities), financial institutions and third parties on how to address the issues identified in the SRC survey and the December 2019 FSB report.

The FSB is inviting comments on this Discussion Paper and the questions set out below. Responses should be sent to fsb@fsb.org by 8 January 2021 with the subject line "Outsourcing and third-party relationships". Responses will be published on the FSB's website unless respondents expressly request otherwise.

1. What do you consider 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?
2. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?
3. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?
4. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

Table of Contents

Executive Summary

Financial institutions (FIs) have relied on outsourcing and other third-party relationships for decades. However, in recent years, the extent and nature of FIs' interactions with a broad and diverse ecosystem of third parties has evolved, particularly in the area of technology. The financial sector's recent response to the COVID-19 pandemic highlights the benefits as well as the challenges of managing the risks of FIs' interactions with third parties, and may have accelerated the trend towards greater reliance on certain third-party technologies. Against this background, this Discussion Paper builds on the FSB's report published in December 2019 on *Third-party dependencies in cloud services* and aims to facilitate a broader discussion on current regulatory and supervisory approaches to the management of outsourcing and third-party risks. The Discussion Paper does not propose any specific principles or standards but rather seeks to promote greater global dialogue among FIs, supervisory authorities and third parties.

The Discussion Paper draws on a survey conducted by the FSB Standing Committee on Supervisory and Regulatory Cooperation (SRC), which asked a series of questions regarding the existing regulatory and supervisory landscape relating to outsourcing and third-party risk management in its member jurisdictions. The survey covered various aspects of the current regulation and supervision of FIs' outsourcing and third-party relationships, including: definitions of outsourcing and third-party relationships; intra-group outsourcing; governance and risk management; data security, information and cyber security; supply chain management; access, audit and information rights; and concentration risk considerations.

The regulation and supervision of FIs' outsourcing and third-party relationships varies across jurisdictions but shares common objectives and principles. For instance, all respondents subscribe to the principle that outsourcing and third-party relationships cannot relieve a FI, its board or senior management from their ultimate accountability for any activities, functions, products or services which they outsource or delegate to a third party. The evolving landscape of FIs' third-party relationships has prompted several supervisory authorities to update or consider updating their regulatory and supervisory framework on outsourcing, third-party risk management and related areas, such as business continuity planning, cybersecurity, data protection, operational resilience and risk management.

All responding supervisory authorities have also set out requirements and/or expectations on how FIs' should manage their outsourcing and third-party relationships. Many have implemented detailed requirements for outsourcing. In some cases, supervisory authorities have implemented additional requirements for third-party relationships deemed critical or important, such as to the safety and soundness of individual FIs or the provision of critical or important functions or critical shared services relevant to financial stability. In addition, in some jurisdictions, supervisory authorities have legal powers giving them some level of access to third parties' data, personnel, premises and systems for the purposes of gathering information relevant to the exercise of their regulatory and supervisory functions. These powers are set out in legislation or regulation, and apply in addition to and independently of any contractual clauses granting access, audit and information rights to FIs and supervisory authorities. They may include the ability to request information directly from third parties relevant to the

authorities' objectives; carry out on-site inspections; and/or supervise the provision of certain third-party services as if they were being performed by the FIs.

Meanwhile, a number of issues and challenges relating to regulatory and supervisory approaches to outsourcing and third-party risk management were also identified. For instance, FIs have to ensure that their contractual agreements with third parties grant to them, as well as to supervisory and resolution authorities, appropriate rights to access, audit and obtain information from third parties. These rights can be challenging to negotiate and exercise, particularly in a multi-jurisdictional context. The management of sub-contractors and supply chains is another challenge that was particularly highlighted in the context of FIs' response to the COVID-19 pandemic. For instance, some FIs experienced delays and logistical difficulties in obtaining remote working equipment from third parties due to disruptions to their global supply chains. Even where contractual arrangements contain provisions and safeguards on the management of the third party's sub-contractors and supply chain, these arrangements often do not bind those sub-contractors directly and can make it difficult for FIs and supervisory authorities to effectively identify and address risks across the supply chain. Another key issue whose importance was highlighted during the COVID-19 pandemic is the importance of implementing appropriate and effective business continuity plans and exit/wind-down plans, to ensure that FIs can recover from an outage or failure at a service provider and, if necessary, exit these arrangements in a way that minimises potential disruption.

Furthermore, there is a common concern among responding authorities about the possibility of systemic risk arising from concentration in the provision of some outsourced and third-party services to FIs. These risks may become higher as the number of FIs receiving critical services from a given third party increases. Potential systemic risk could arise if, for instance, a sufficiently large number of FIs (or a single systemic FI) became dependent on one or a small number of outsourced or third-party service providers for the provision of critical services that were impossible or very difficult to substitute effectively and in an appropriate timeframe. Where there is no appropriate mitigant in place, a major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple FIs.

While mapping and understanding the system-wide effects of third-party dependencies is not a new issue, it remains an evolving area for supervisory authorities due to the heterogeneity of services provided and the changing ecosystem. Given the cross-border nature of this dependency, supervisory authorities and third parties could particularly benefit from enhanced dialogue on this issue.

Introduction

Financial institutions (FIs)[1] have relied on outsourcing and other third-party relationships for decades.[2] However, in recent years, the extent and nature of FIs' interactions with a broad and diverse ecosystem of third parties has changed, particularly in the area of technology. The FSB's report published in December 2019 on *Third-party dependencies in cloud services* explored potential issues for supervisory authorities and financial stability stemming from the scale of services provided via the cloud and the small number of globally dominant players providing such services.[3] It concluded that further discussion on current approaches to the management of outsourcing and third-party risks would be useful.

Outsourcing and other third-party relationships can bring multiple benefits to FIs, including: enhanced operational resilience; faster and more tailored financial products and services; cost reduction; greater innovation; and improved internal processes. They can also bring increased benefits to small and medium FIs that often lack the scale of larger FIs, particularly in technology investment. However, outsourcing and third-party relationships can give rise to new or different risks to FIs and potentially to financial stability that need to be adequately managed. Some of the measures that FIs and supervisory authorities have introduced in response to the COVID-19 pandemic have highlighted the opportunities and risks that outsourcing and third-party relationships can create for the financial sector. Some third-party information and communication technology (ICT) providers have been vital facilitators of the mass, global transition to remote working during the pandemic and, by extension, the continuous provision of services to FIs' clients from a range of locations. FIs have been able to leverage the scalability and resilience of certain third-party service providers to quickly implement new working patterns with relatively little disruption to the provision of critical services. At the same time, FIs' response to the pandemic may have accelerated their reliance on some third parties, possibly exacerbating some authorities' concerns about third-party risks, in particular, concentration risk. Moreover, the financial resilience of some third parties might be tested in a severe, prolonged economic downturn. The FSB also stated that disruption to telecoms or third-party service providers could affect FIs in its recent assessment of the financial stability implications associated with COVID-19.[4]

The FSB Standing Committee on Supervisory and Regulatory Cooperation (SRC) conducted a survey of the existing regulatory and supervisory landscape relating to outsourcing and third-party risk management in its member jurisdictions.[5] The survey covered various aspects of the

---

1 For the purpose of this discussion paper, financial institutions include: banks, insurers, financial market infrastructures, trading venues or exchanges, broker-dealers, asset managers, and pension funds among others.

2 FIs rely on third parties for a number of services, ranging from traditional functions, such as accounting, external audit or human resources to the development of innovative financial products. Third-party relationships include any business arrangement between a FI and another entity by contract or otherwise, such as activities that involve outsourced product or services, use of independent consultants, networking arrangements, merchant payment processing, services provided by affiliates and subsidiaries, and joint ventures.

3 FSB (2019) *Third-party dependencies in cloud services: Considerations on financial stability implications*, 9 December.

4 FSB (2020b) *COVID-19 pandemic: Financial stability implications and policy measures taken*, 15 April 2020.

5 They are: Argentina, Australia, Brazil (BCB), Canada (OSFI), China (CBIRC), France, Germany, Hong Kong, Italy, Japan (JFSA), Korea (FSC), Mexico (CNBV), the Netherlands, Russia (Bank of Russia), Saudi Arabia (SAMA), Singapore (MAS), South Africa (SARB, FSCA), Spain, Sweden (FSA), Switzerland (FINMA), Turkey (CMBT), UK (BoE, FCA) the US, and the EU (EC-ECB-ESAs). Some responses only represent the views of responding supervisory authority as opposed to all financial supervisory authorities in that jurisdiction (e.g. Capital Markets Board of Turkey (CMBT) for Turkey).

current regulation and supervision of FIs' outsourcing and third-party relationships, including: governance and risk management; cyber, data and information security; access, audit and information rights; and business continuity planning and exit strategies. A detailed overview of responses to the SRC survey is included in the Annex.

Drawing on the responses to the survey, this discussion paper:

- provides a high-level overview of the existing regulatory and supervisory landscape based on the survey findings as well as some preliminary observations from authorities' and FIs' recent responses to the COVID-19 pandemic (Section 1);
- briefly describes various regulatory and supervisory approaches for managing outsourcing and third-party risks in SRC member jurisdictions (Section2);
- lists some common regulatory and supervisory challenges (Section 3); and
- identifies issues for further exploration (Section 4).

This discussion paper seeks to encourage dialogue among FIs, supervisory authorities and third parties on challenges in identifying and managing the risks relating to their outsourcing and third-party dependencies. It also sets out some additional issues relating to outsourcing and third-party risk management in the financial sector which the COVID-19 pandemic has highlighted to invite views from FIs and third parties.

1. Overview of existing regulatory and supervisory landscape on outsourcing and third-party relationships[6]

The regulation and supervision of FIs' outsourcing and third-party relationships varies across jurisdictions but shares common objectives and principles. Most jurisdictions have longstanding regulatory requirements and/or supervisory expectations on outsourcing and/or third-party risk management.[7] In recent years, there has been an increasing use and dependency by FIs on ICT solutions and tools provided by or through third parties. This evolving landscape has led several supervisory authorities to update or consider updating their regulatory and supervisory framework on outsourcing, third-party risk management and related areas, such as business continuity planning, cybersecurity, data protection, operational resilience and risk management.[8]

---

6 For a brief overview of international standards and initiatives related to outsourcing and third-party relationships, see Section 5 of FSB (2019).

7 In general, "jurisdictions", "authorities" and "supervisory authorities" used in this discussion paper refer to those responded to the SRC survey (see footnote 6).

8 For example, in the EU, the European banking Authority (EBA) issued guidelines on outsourcing arrangements and on ICT and security risk management that are designed to promote a harmonised, level-playing field in the EU banking sector. For details, see EBA (2019a) *Guidelines on outsourcing arrangements*, February and EBA (2019b) *Guidelines on ICT and security risk management*, November. At the international level, the International Organization of Securities Commissions (IOSCO), for example, issued its proposed updates to its Principles on Outsourcing for public consultation in May 2020 that comprise a set of fundamental precepts and a set of seven principles for regulated entities that outsource tasks to service providers. See IOSCO (2020) *Principles on Outsourcing: Consultation Report*, May.

For instance, all respondents subscribe to the principle that outsourcing and third-party relationships cannot relieve a FI, its board or senior management from their ultimate accountability for any activities, functions, products or services which they outsource or delegate to a third party. All supervisory authorities rely primarily on FIs to manage the risks in their outsourcing and third-party relationships. They do so through regulatory requirements and supervisory expectations regarding how FIs should oversee these relationships, with a particular focus on those that are critical or important to financial stability; the safety and soundness of FIs; or the provision of critical or important functions. FIs have to ensure that their contractual agreements with third parties do not impair their ability to meet their regulatory obligations. These regulatory requirements often include requirements on FIs to ensure that their contractual arrangements with third parties grant them and their regulators rights to access, audit and obtain information from those third parties. While several supervisory authorities have specific requirements or expectations on the management of risks that may arise in a third party's sub-contractors or its supply chain, contractual arrangements typically only bind the FI and the third party but not fourth, fifth parties and beyond. A number of supervisory authorities see this as a significant limitation on the ability of FIs to manage risks across the supply chain, and expect FIs have adequate visibility of their third parties' supply chain.

In some jurisdictions, supervisory authorities have legal powers giving them some level of access to third parties' data, personnel, premises and systems for the purposes of gathering information relevant to the exercise of their regulatory and supervisory functions. These powers are set out in legislation or regulation, and apply in addition to and independently of any contractual clauses granting access, audit and information rights to FIs and supervisory authorities. They may include the ability to request information directly from third parties relevant to the authorities' objectives; carry out on-site inspections; and/or supervise the provision of certain third-party services as if they were being performed by the FIs. Section 2 describes and provides examples of the powers available to some financial supervisory authorities.

The SRC survey identifies a range of issues and challenges relating to outsourcing and third-party risk management:

- *Regulatory scope:* Most supervisory authorities have adopted definitions of "outsourcing" that are broadly consistent with the definition in the 2005 Joint Forum report on *Outsourcing in Financial Services*.[9] However, in this definition and in some jurisdictions' regulatory requirements or supervisory expectations, the term "outsourcing", as defined in their current regulatory standards, may not capture all third-party relationships with a potential impact on financial stability or the safety and soundness of FIs. Some jurisdictions and international bodies, such as the G7, have broadened or are considering broadening the scope of their regulatory framework or principles-based approach to all "third-party relationships" that can pose risks to FIs or financial stability.[10] For instance, the Basel Committee on Banking Supervision's

9 Joint Forum (2005) *Outsourcing in Financial Services*, February

10 For example, see G7 (2018) *G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*, 24 October.

(BCBS) August 2020 consultative document on *Principles for operational resilience*[11] applies to all dependencies on banks' relationships with third parties or intra-group entities relevant to the delivery of "critical operations". The nature of these "third-party relationships" can vary. For example, they may include certain purchases of critical hardware or software from third-party vendors.[12] However, "outsourcing" remains an important subset of the wider range of third-party relationships".

- *Information technology (IT) outsourcing*: Supervisory authorities are responding to FIs' evolving use on technology solutions provided by third parties. In particular, they are trying to address the risks and harness the benefits of the cloud, which the BCBS describes as an "enabling technology" that provides the underlying infrastructure for many FinTech activities and other technology solutions, such as advanced analytics.[13] Most jurisdictions consider the use of cloud computing as a form of outsourcing and some have clarified their regulatory requirements and supervisory expectations relating to FIs' use of the cloud by:

  (i) issuing standalone cloud-specific policies; or

  (ii) including specific references to or sections on cloud in their overall policies on outsourcing and third-party risk management, cybersecurity and/or IT.

- *Data protection*: Many jurisdictions have recently introduced or plan to introduce new or revised regulatory requirements relating to the protection of data that FIs transfer to or share with third parties. These requirements complement and intersect with national or regional legal regimes on the protection of personal data that apply across all sectors, not just financial services.

- *Access, audit information rights*: In most jurisdictions, FIs have to ensure that their contractual agreements with third parties grant to them, as well as to supervisory and resolution authorities, appropriate rights to access, audit and obtain information from those third parties. However, these rights can be difficult to negotiate and exercise in practice. For instance, where relevant data or a third party's premises are located in multiple jurisdictions conflicting legal and regulatory approaches and/or logistical or other issues may cause delays or difficulties to the ability of supervisory authorities to access relevant information, thereby impeding the effective exercise of their supervisory functions.

- *Supply chain management*: Notwithstanding the existence of specific requirements and supervisory expectations on sub-outsourcing in many jurisdictions, managing the risks in the complex supply chains involved in some outsourcing and third-party agreements can be difficult in practice. Even where contractual arrangements contain provisions and safeguards on the management of the third party's sub-contractors and supply chain, these arrangements often do not bind those sub-contractors directly and

---

11 BCBS (2020) *Principles for operational resilience*, 6 August

12 For example, the Eurosystem as payment systems overseer focuses on those third parties that are critical to the core functioning of FMIs.

13 BCBS (2018), *Sound Practices: implications of fintech developments for banks and bank supervisors*, 19 February

can make it difficult for FIs and supervisory authorities to effectively identify and manage risks across the supply chain.

Jurisdictions and FIs' responses to COVID-19 illustrate the opportunities and highlight the challenges of managing the risks that outsourcing and third-party relationships pose for the financial sector. The FSB has emphasised that "disruption to telecoms or third-party service providers could also affect financial institutions" and highlighted the importance of "ensuring that external service providers and/or critical suppliers are taking adequate measures and are sufficiently prepared for a scenario in which there will be heavy reliance on their services". The FSB has also highlighted the importance of (among others) third-party providers who deliver core services being treated as "essential personnel" so that a limited number of staff necessary to operate critical functions may be required to remain on-site during the pandemic as opposed to being able to work remotely.[14]

Other supervisory authorities and SSBs have set out consistent expectations, for example as follows:

- The US Federal Financial Institutions Examination Council (FFIEC), on behalf of its member agencies, has emphasised that "open communication and coordination with third parties, including critical service providers, is an important aspect of pandemic planning" and urged FIs' management to "monitor its service providers, identify potential weaknesses in the service and supply chains, and develop potential alternatives for obtaining critical services and supplies".[15]

- The National Association of Insurance Commissioners (NAIC) adopted a model law addressing data security, which a number of US states have adopted. That law requires insurers to design an information security program to mitigate identified risks, including their use of third-party service providers. It also requires insurers to (i) exercise due diligence in selecting third-party service providers; and (ii) require their third-party service providers to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and non-public information.[16]

- The European Central Bank (ECB) has urged FIs to enter into "a dialogue with critical service providers to understand whether and to ascertain how services continuity would be ensured in case of a pandemic".[17]

- The Japanese Financial Services Agency (JFSA) and the Bank of Japan published in April 2020 a joint notification asking FIs to update their contact list of stakeholders, including IT and telecommunications vendors, and reconfirm their procedure for incident response. In addition, in order to continue their business if third-party staff are infected, FIs were recommended to socially distance from vendors and reorganise their teams to improve their business continuity and resilience.

---

14 FSB (2020a) *Press Release: FSB members take action to ensure continuity of critical financial services functions*, 2 April

15 FFIEC (2020) *Interagency statement on Pandemic Planning*, March

16 NAIC (2017) *Insurance Data Security Model Law* (#668), 4th Quarter

17 ECB (2020) *Contingency preparedness in the context of COVID-19*, 3 March

- The Central Bank of Brazil (BCB) strengthened its relationship with the Brazilian telecommunications regulator due to the increased dependence of FIs on communication services during the COVID-19 pandemic. The regulators are thus, discussing potential emerging risks to the financial system arising from telecom providers.

FIs' responses to COVID-19 has shone a light on a number of issues relating to third-party risk management, including:

- the importance of understanding the ability and capacity of third parties (and the capacity, availability and resilience of third-party technology) to remain resilient in challenging economic and operational environments, and continue to adequately provide or support critical functions in FIs;

- a heightened focus on safeguarding confidential and sensitive data at a time when employees are working from home and increasingly relying on third-party technology solutions;

- the importance of identifying, monitoring and managing risks across the supply chain (e.g. in sub-contractors providing critical products or services to a third party), in particular, where the supply chain is spread across jurisdictions, including major offshore hubs;

- the importance of implementing effective business continuity plans to ensure that FIs can recover from an outage or failure at a service provider; and

- the importance of having a feasible exit plan (e.g. by carrying out an analysis of the potential cost and timing implications of transferring an outsourced service to an alternative provider or reincorporating the service in-house).

2. Supervisory approaches for managing outsourcing and third-party risks

All supervisory authorities have set out requirements and/or expectations regarding FIs' outsourcing and third-party relationships. Many have implemented detailed requirements for outsourcing and, in some cases, other third-party relationships deemed critical or important to financial stability, the safety and soundness of FIs or the provision of critical or important functions or critical shared services. These include requirements for FIs to:

- put in place adequate governance and internal controls to manage third-party risks; and

- ensure that their arrangements with third parties allow FIs to comply with their legal and regulatory obligations, and manage any risks that the arrangement may pose to FIs or to their customers.

In some jurisdictions supervisory authorities have been granted legal powers giving them some level of direct access or oversight over relevant activities provided by third parties, which enables supervisory authorities to:

- request certain information directly from third parties (e.g. information relating to their relationships with regulated FIs or information that the supervisory authority considers might be relevant);
- conduct on-site inspections at third parties;
- supervise services provided to FIs by third parties as if they were being performed by the FIs themselves; or
- bring third parties meeting certain criteria into their direct supervisory remit.[18]

Legal powers granting supervisory authorities direct access to third parties where they exist tend to be limited to third parties that: (i) provide services to specific types of FI, such as banks or systemically important FIs (e.g. systemically important payment systems); and (ii) meet specific criteria, often relating to the criticality or importance of the services they provide.

Some SRC member jurisdictions provide for a legal power granting supervisory authorities direct supervisory recourse to third parties and the ability to request information directly from those third parties. These powers do not, however, have the effect of making third parties supervised institutions. For instance:

- The Australian Securities and Investment Commission (ASIC) has compulsory information-gathering powers and can compel local third parties to provide documents relevant to an Australian Financial Services Licensee.
- The European Securities and Markets Authority (ESMA) can request information from and conduct general investigations and on-site inspections at third parties to whom non-European Economic Area (EEA) central clearing counterparties (CCPs) and trade repositories that are recognised and registered in the EU have outsourced operational functions or activities.
- The UK Prudential Regulation Authority (PRA) can require service providers to provide it with information it considers "is or might be, relevant to the stability of the UK financial system".
- The Capital Markets Board of Turkey (CMBT) has similar legal powers over the service providers of portfolio management companies and investment firms.

In some jurisdictions authorities have powers to conduct on-site examinations. For example,

[18] In n Luxembourg, certain service providers to FIs are required to be approved and supervised by the CSSF as "'Professionals of the Financial Sector'" (locally abbreviated to PSFs). There are multiple categories of PSF, including "'Primary IT systems operators'" and '"Secondary IT systems and communication networks operators"'.

- The Australian Prudential Regulatory Authority (APRA) has information gathering authority, as well as the right to conduct on-site visits to the service providers if APRA considers it necessary in its role as a prudential supervisor. Outsourcing standard CPS231 requires these rights to be formalised in the outsourcing agreement.[19]

- The ECB Single Supervisory Mechanism (SSM) can carry out on-site inspections on "third parties to whom SSM-supervised entities have outsourced functions or activities".[20] Moreover, the ECB in its payment systems oversight function can request information and carry out on-site inspections of critical service providers of systemically important payment systems, but only subject to a contractual provision between the system and service provider allowing for this.

- The Bank of Italy has legal powers to "require information and conduct inspections of service providers to which essential or important functions are outsourced".

- The US Bank Service Company Act gives federal banking agencies the authority to conduct examinations of certain bank services provided by third parties to the same extent that they would be examined if they were being provided in-house by FIs. The Bank Service Company Act applies only to third-party services provided to US depository institutions (i.e. banks), and not to third-party services provided to non-bank FIs. The services covered under the Bank Service Company Act include banking-related functions that a bank may perform by itself, such as account processing. The Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve, the Consumer Financial Protection Bureau, and National Credit Union Administration (along with a state liaison) have developed an inter-agency programme for supervising relevant service providers as a coordinated way to exercise their respective authorities over third parties.

- In the UK, HM Treasury (HMT) has the power to bring certain service providers to recognised payment system operators (RPSOs) overseen by the Bank of England (BoE) into the BoE's supervisory remit by designating them as "specified" service providers. HMT may do so, upon a recommendation from the BoE, if it considers that a service provider to a RPSO is systemically important to UK financial stability. For instance, if that service provider provides critical services to a payment system that is itself systemically important. The BoE's powers over "specified" service providers are similar to those it has over RPSOs. The BoE's approach to supervising "specified" service providers draws upon Annex F of the CPMI-IOSCO Principles for financial market infrastructures (FMIs), which sets out oversight expectations applicable to critical service providers.[21]

- In Belgium, the National Bank of Belgium (NBB) directly oversees SWIFT in accordance with standards aligned with Annex F of the CPMI-IOSCO Principles for

---

19 APRA (2017) *Prudential Standard CPS 231 Outsourcing*, July.

20 This power does not cover all the global operations or premises of service providers to whom FIs have outsourced their functions or activities, and only those in jurisdictions within the SSM's remit or where the agreement allows the SSM to do it.

21 CPMI-IOSCO (2012) *Principles for Financial Market Infrastructures* , April

FMIs, known as the "High level expectations for the oversight of SWIFT". SWIFT oversight is built on a mechanism for supervisory cooperation comprising the central banks of the G10 jurisdictions and a SWIFT Oversight Forum comprising a wider range of banks. [22]

These kinds of powers of authorities can enhance the ability of supervisory authorities to monitor certain risks and how they are managed. They can complement, and are not instead of and do not replace, the primary responsibility of FIs for managing the risks in their outsourcing and third-party relationships as replacing this responsibility could give rise to moral hazard and potential confusion as to the respective roles of FIs and supervisory authorities. In certain cases, such as where relevant data or a third party's premises are located in multiple jurisdictions, differences in legal and regulatory approaches and/or logistical or other issues may cause delays or difficulties to the ability of supervisory authorities to access relevant information, thereby impeding the effective exercise of their supervisory functions. Against this background, cross-border regulatory and supervisory dialogue and cooperation in this area is becoming increasingly important.

3. Regulatory and supervisory challenges

Some common key challenges faced by supervisory authorities include:

(i) practical limitations on their ability to ensure that FIs appropriately manage the risks in their outsourcing and third-party agreements (including risks in the third party's wider supply chain);

(ii) limitations on their ability to effectively oversee supervised FIs' outsourcing and third-party arrangements in a cross-border context; and

(iii) challenges in identifying, monitoring and managing potential systemic risks related to FIs' use of outsourcing and third-party arrangements, in particular, due to concentration in the provision of third-party services and lack of relevant information.

3.1. Practical challenges

3.1.1. Shortage of relevant resources, and ICT skills

A general supervisory challenge flagged in several responses to the SRC survey is assuring that FIs have appropriate resources and skills to effectively address outsourcing and third-party risks, in particular where these rely on complex and constantly evolving ICT solutions that are not necessarily specific to FIs, and that supervisory and resolution authorities have appropriate resources for oversight as well. Recruiting, retaining and training employees with

[22] The oversight approach is based on moral suasion as distinct from the more prescriptive forms of regulation and supervision that FIs are subject to. While a Financial System Stability Assessment of Belgium undertaken by the International Monetary Fund (IMF) found the approach to be effective, it is being challenged by evolving risks, including cybersecurity incidents at SWIFT's customers (See IMF (2018), *Belgium Financial System Stability Assessment*, 6 March). Meanwhile, to mitigate the related risks, SWIFT has established its Customer Security Programme (CSP) that would support its customers in fighting cyber-attacks.

the relevant experience and skills to effectively manage the growing range of third-party ICT providers is a challenge for FIs as well as for supervisory and resolution authorities overseeing them.

3.1.2. Limitations on access, audit and information rights

Supervisory authorities have issued requirements or guidance to FIs to ensure that their outsourcing or third-party contractual agreements give FIs, supervisory and resolution authorities and persons appointed on their behalf (e.g. external auditors) appropriate[23] access to relevant data, information, premises, personnel and systems at the third party ("'access, audit and information rights"). There is consensus across the respondents that access, audit and information rights should, as a minimum, allow:

- FIs to obtain the necessary assurance that the third party is delivering the relevant activity, function, product or service in line with the FIs' regulatory obligations; and
- resolution and supervisory authorities to effectively perform their statutory functions.

Responses to the SRC survey highlighted certain challenges and issues relating to the ability of FIs to negotiate and exercise appropriate access, audit and information rights in outsourcing and third-party arrangements, both for FIs and for their supervisory and resolution authorities. In particular, respondents noted that:

- third parties are sometimes unaware of the regulatory obligations of their FI clients or face difficulties in facilitating compliance with them. Imbalances in the respective negotiating power of FIs and third parties can also impact on the ability of FIs to exercise effective oversight.
- continuous individual on-site audits can also create challenges for third-party service providers. For instance, in terms of the resources required to plan and execute these audits and their potential impact on other clients of the same provider.[24]
- even where third parties are aware of the regulatory obligations of their FI clients, they may refuse to grant their FI clients (and their supervisor) access to their premises for different reasons (e.g. they can face difficulties in facilitating compliance with them, or their predominant position on the market allows them to reject external audit demand from their FI clients).
- even where FIs as well as supervisory and resolution authorities have adequate access, audit and information rights (and/or direct supervisory recourse to third parties), they may have limited tools to compel a third party to remedy any issues they may identify. If resolution of identified deficiencies is not possible through contractual mechanisms, which FIs are primarily responsible for raising with third parties,

---

[23] The language used by supervisory authorities to describe how extensive access, audit and information rights varies across jurisdictions and ranges from "adequate" and "effective" to "unrestricted".

[24] Third-party providers may offer audit report on their own services to their FI clients to compensate for the on-site audits by their FI clients, but, depending on the content, level of detail and quality of these reports, they may not always be sufficient to allow their FI clients to comply with their regulatory obligations in terms of third-party risk management.

supervisory and resolution authorities may carry the deficiencies over into the supervisory assessment of the regulated FI. In some scenarios, these deficiencies may also result in the FI terminating the arrangement.

There are emerging practices that seek to make the exercise of access, audit and information rights more effective and efficient. For instance:

- the provision of certificates and reports by third parties evidencing compliance with recognised standards (e.g. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)). It is, however, important that individuals with appropriate relevant expertise in FIs review the information in these reports and scrutinise the adequacy of the assurance provided. Undue reliance on the existence of these attestations and reports without further scrutiny is not enough to provide the necessary assurance to FIs.

- audits by groups of FIs sharing common third parties and performed by representatives of the FIs or specialists appointed on their behalf (known as "pooled audits"). While pooled audits can constitute a more effective and proportionate method of obtaining assurance from third parties, senior management in FIs should still review the conclusions of any collective reports and assess what such collective conclusions mean to their individual institutions, rather than treating them as a mechanical exercise.

3.1.3. Supply chain management

Although there are regulatory requirements and supervisory expectations specifically relating to the management of sub-contractors ("nth parties") and supply chains in several jurisdictions, a number of SRC survey responses highlighted the limitations in the abilities of both FIs and supervisory authorities to identify these "nth-party risks" as a practical challenge.

In particular, some respondents noted that the ability of a contractual arrangement between a FI and a third party to bind or influence that third party's sub-contractors is limited and decreases the longer and more complex the supply chain becomes.

3.2. Cross-border challenges

Challenges relating to the exercise of access, audit and information rights can be more pronounced where third parties provide services from a foreign jurisdiction. Such challenges include the following:

- Even in those jurisdictions where supervisory and resolution authorities have powers giving them some level of direct access to third parties, this access may not be exercisable on a cross-border basis in the absence of strong contractual safeguards and/or mechanisms for supervisory cooperation. In this scenario, it is particularly important for FIs as primarily responsible for managing the risks in their third-party arrangements to obtain appropriate assurance that any cross-border elements in these arrangements will not prevent them from meeting applicable jurisdictions' legal or regulatory obligations. Access to a third party in another jurisdiction by the relevant

authorities, without creating unnecessary burden, conflict or duplication, is a challenge that could be addressed by establishing cross-border supervisory cooperation and coordination mechanisms.

- Supervisory and regulatory challenges can arise due to differing (or the lack of) data confidentiality standards and regulations that could hamper the sharing of information and an efficient data management policy relating to the outsourced or third-party services in a foreign jurisdiction.

- Cross-border complexities can give rise to challenges for resolution authorities in particular, as they may limit their ability to exercise step-in rights in resolution, especially when critical data or systems are held in a foreign jurisdiction, or where the service providers enter insolvency proceedings in a foreign jurisdiction. In this regard, the FSB offers guidance to help authorities ensure firms that are subject to resolution planning requirements have appropriately robust outsourcing arrangements for critical shared services in the case that a firm enters resolution.[25]

Mitigants to address these challenges continue to evolve. Regulatory approaches to cross-border data access, audit and information rights may also vary among regulators and by sector, each with varying trade-offs. For example, some approaches to minimise these cross-border challenges could encourage market fragmentation, possibly resulting in negative effects on FIs' capabilities and resilience. FIs in different sectors may use third parties in significantly different ways and may take different approaches to meet challenges related to access, audit and information rights as part of their cross-border risk management practices. Further analysis and discussion of the benefits and costs of different approaches, or discussion on developing new approaches to addressing these cross-border challenges, as they emerge, would be beneficial.

3.3. Potential systemic risks

A common concern among respondents to the SRC survey is the possibility of systemic risk arising from concentration in the provision of some outsourced and third-party services to FIs. These risks may become higher as the number of FIs receiving critical services from a given third party increases.

Systemic risk could arise if, for instance, a sufficiently large number of FIs (or a single systemic FI) became dependent on one or a small number of outsourced or third-party service providers for the provision of critical services that were impossible or very difficult to substitute effectively and in an appropriate timeframe, for instance due to limitations in the capacity of alternative third parties or other back-up solutions. A major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple FIs. The ultimate impact would depend on the specific services being provided, the criticality and substitutability of those services, and the mitigation plans in place by FIs and the third party in question. Industry practice on mitigation plans is evolving rapidly and encompasses an ever-growing range of

[25] For details, see FSB (2016) *Guidance on Arrangements to Support Operational Continuity in Resolution*, August.

contractual, practical and technological approaches. For instance, retaining the ability to bring data or applications back on-premises in a way that ensure continuous adequate performance; creating and securing back-up copies of sensitive data, using of multiple or back-up vendors or, in the case of cloud outsourcing, using one or more resilience options.

While mapping and understanding the system-wide effects of third-party dependencies is not a new issue, it remains an evolving area for supervisory authorities due to the heterogeneity of services provided and the changing ecosystem. Given the cross-border nature of this dependency, supervisory authorities and third parties could particularly benefit from enhanced dialogue on this issue.

4. Conclusion

Supervisors and resolution authorities are increasing their focus on issues arising from developments in technology and a greater pursuit of digital transformation strategies, often involving a growing range of third-party providers, including technology providers. Arrangements between FIs and third parties can have undeniable benefits for FIs, including the ability to improve their resilience (and reduce some risks), innovate and reduce costs. At the same time, they can also amplify or transform other risks and possibly create new ones, if managed ineffectively.

The high pace of evolution of third-party relationships, including where and how FIs use third-party providers, can make understanding and managing these risks more complex. Additional analysis may be considered to better understand the risks posed by the changing landscape of outsourcing and third-party relationships, and whether existing approaches allow FIs to capture the benefits while sufficiently address the risks that outsourcing and third-party relationships may pose to FIs and, potentially, to financial stability.

Effective cross-border cooperation and dialogue among supervisory authorities as well as the effective application of existing standards and other emerging practices are important to address these challenges and risks.

Annex: Regulatory and supervisory approaches to outsourcing and third-party relationships based on SRC survey responses

Regulatory standards on outsourcing and/or third-party relationships (or their risk management) can be set out in primary legislation, principles, rules or guidance issued by the relevant regulatory or supervisory authorities (hereafter authorities), codified supervisory practices and any combination thereof.

Requirements and regulatory/supervisory expectations on outsourcing and third-party risk management issued by the relevant authorities are generally addressed to FIs and require them to ensure that their written agreements with third-party service providers allow them to meet their regulatory obligations and manage risks to the relevant FI and to their customers.

- EU and its member state authorities follow a rules-based approach based on harmonised EU legislation, such as Markets in Financial Instruments Directive (MiFID) II for markets in financial instruments and Solvency II for insurers, supplemented by definitions of outsourcing and third-party relationships. In addition, Guidelines for FIs exist, such as the European Banking Authority (EBA) *Guidelines on Outsourcing Arrangements* published in February 2019, [26] the European Insurance and Occupational Pensions Authority (EIOPA) *Guidelines on outsourcing to cloud service providers* published in January 2020[27] and national laws or circulars.

- Certain authorities in the US tend to issue principles-based regulations and supplement them with guidance in, for instance, circulars, letters and explanations of supervisory practices. In addition, certain US agencies also have the legal authority to directly supervise specific services provided to banks by third-party providers. Their supervisory authority is nevertheless limited to the services being provided to deposit-taking institutions rather than the full oversight or supervision of the third-party entities providing the services.

- Many jurisdictions and/or supervisory authorities follow a similar rules-based approach (e.g. Brazil, Saudi Arabia, South Africa, Turkey) or guidance-based approach (e.g. Hong Kong). Requirements on outsourcing and third-party risk management are normally consistent with and complemented by wider requirements on areas such as business continuity, corporate governance, information security or risk management. Arrangements with a cross-border element may sometimes be subject to enhanced or additional requirements (e.g. on information security).

- Some authorities have historically relied on principles-based guidance but are intending to introduce “legally binding requirements”. For example, the Monetary Authority of Singapore (MAS) published a principles-based guidance in 2004, which has undergone revisions since, and recently introduced proposals for legally binding

[26] EBA (2019a) *Guidelines on outsourcing arrangements*, 25 February

[27] EIOPA (2020) *Guidelines on outsourcing to cloud service providers*, January

requirements for banks and merchant banks in relation to their material outsourcing arrangements.[28]

1. Definitions of outsourcing and third-party relationships

There is considerable variance in how surveyed authorities define "outsourcing" and "third-party relationships", or indeed in whether they define these terms at all.[29] Most surveyed authorities do have a definition for "outsourcing", but do not explicitly define "third-party relationships" or "third-party arrangements".

1.1. Outsourcing

Many of the existing supervisory authorities' definitions of "outsourcing" appear to have a common origin namely the February 2005 report issued by the Joint Forum on *Outsourcing in Financial Services* (Joint Forum Guidelines).[30] The definition of outsourcing in the Joint Forum Guidelines is "a regulated entity's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future".

The Joint Forum's definition of "outsourcing" for example provides the foundation for the definition in the EU including the MiFID II; the Solvency II Directive and the 2019 EBA Guidelines on outsourcing arrangements.

While the definition of "outsourcing" in most jurisdictions is consistent, there are variations such as the following.

- Some jurisdictions consider all types of activities that a FI could perform itself as "outsourcing".
- Conversely, other jurisdictions have a more targeted definitions of "outsourcing" encompassing, for instance, activities directly linked to the provision of financial services. For example, the Korean Financial Services Commission (FSC) defines "outsourcing" as the practice of:
  - utilising third-party facilities or human resources to operate authorised business of FIs; and
  - third-party contracting for information processing.
- In some jurisdictions, such as Russia, Singapore or Switzerland, only continuous or recurrent arrangements between FIs can be considered "outsourcing". In Russia, only

---

28 MAS (2019) *Consultation Paper on Outsourcing by Banks and Merchant Banks*, February

29 Standards by SSBs have a similar level of heterogeneity.

30 Joint Forum (2005) *Outsourcing in Financial Services*, February

continuous arrangements relating to the "full transfer of the business function" come under the definition of "outsourcing".

- IOSCO's proposed updates to its *Principles on Outsourcing*, which were issued for public consultation in May 2020, define "outsourcing" as a business practice in which a regulated entity uses a service provider to perform tasks, functions, processes, services or activities (collectively, "tasks") that would, or could in principle, otherwise be undertaken by the regulated entity itself.[31] IOSCO further clarifies that outsourcing may include tasks that the regulated entity has not previously performed, where those tasks would reasonably be expected to be initiated by the regulated entity if they had not been outsourced to a third party and tasks that the regulated entity does not have the capacity or resources to perform. This may occur in particular when a new regulated entity is established, or when an existing regulated entity enters a new area of business or becomes subject to a new regulatory requirement.

Most authorities consider arrangements with cloud service providers a form of "outsourcing". For instance, in Japan, "outsourcing" is defined as use of an outside service provider, including a shared data centre and a cloud service provider, to perform system development, system operation or information processing. Some jurisdictions such as Australia, Brazil and Korea, have issued specific guidance or provisions for the management of cloud outsourcing arrangements. The scope of the Brazilian Financial System Regulation includes all relevant services for data processing and storage, which is broader than cloud services. For instance, it may include services related to primary data sent for processing at credit risk bureaus if the FI considers it a critical service.

1.2. Third-party relationships

Most authorities do not currently have explicit requirements or supervisory expectations for third-party arrangements other than "outsourcing". However, some authorities do define and apply consistent supervisory expectations to all "third-party relationships". For example, the US Office of the Comptroller of the Currency (OCC) defines it broadly as "any business arrangement between a bank and another entity, by contract or otherwise" including partnerships or joint ventures with external parties.[32]

The BCB in Brazil does not explicitly define "outsourcing" or "third-party arrangement" as such but uses related term that are comparable to third-party and outsourcing arrangements in its scope.

In Argentina, the term "third-party relationship" is an umbrella term for "outsourcing" and the provision of services to a FI by another entity in its group but located in another jurisdiction (referred to as "offshoring" in some jurisdictions).

---

31 IOSCO (2020) *Principles on Outsourcing: Consultation Report*, May

32 OCC (2020) *Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, 5 March

There is an emerging trend whereby some authorities appear to be gradually moving away from the definition of "outsourcing" and towards a more holistic notion of "third-party arrangement" (of which outsourcing is a subset). This is evidenced by the recent:

- G7 *Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector*, which apply to all third parties, defined as "organizations that have entered into business relationships or contracts with an entity to provide a product or service". [33]

- EBA *Guidelines on Information and Communications Technology (ICT) and Security Risk Management*, which apply to all arrangements which credit institutions, investment firms, payment institutions and e-money institutions may enter into with "third parties" (defined in the same way as in the G7 document above), such as hardware and software purchases.[34]

- The BCBS in its August 2020 consultative document on *Principles for operational resilience* also uses the wider concept of 'third-party dependency management' and notes that "banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations".[35] The BCBS' August 2020 consultative document on revised *Principles on the sound management of operational risk* also includes principles-based guidance on the management of third-party arrangements.[36] The term critical operations in the BCBS principles references FSB guidance, and encompasses the term "critical functions".[37]

- The consultation paper (CP) on *Outsourcing and third-party risk management* published by the PRA (CP30/19), which sets out the UK PRA's proposals for a modernised regulatory framework on outsourcing and third-party risk management.[38] CP30/19 seeks feedback on, among other areas, the ongoing appropriateness of the existing definition of "outsourcing" and whether a new definition of third-party relationships aligned to the G7 definition should be introduced.

- FSB *Guidance on Arrangements to Support Operational Continuity in Resolution* calls for a clear mapping between critical shared service[39] providers and recipients.[40] This mapping should include relevant details such as the jurisdiction of each party; description of the service; and which of the service delivery models is being used. This mapping should also include services provided between critical shared service providers, if relevant (e.g. an intra-group service company sub-contracting with a third-

---

33 G7 (2018) *Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector*, 15 October

34 EBA (2019b) *Guidelines on Information and Communications Technology (ICT) and Security Risk Management*, 29 November

35 BCBS (2020) *Principles for operational resilience: Consultative Document*, August

36 BCBS (2020) *Revisions to the principles for the sound management of operational risk*, August

37 FSB (2013) *Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services*, 16 July

38 PRA (2019) *Outsourcing and third party risk management*, December

39 For a definition of critical shared services, see the FSB (2013) *Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on the Identification of critical functions and critical shared services*, 16 July.

40 FSB (2016) *Guidance on Arrangements to Support Operational Continuity in Resolution*, August.

party service provider). The FSB Guidance also recommends the use of service level agreements that provide for continuity of the covered services in resolution and sets out guidance on the contractual provisions that could be included.

- The CPMI-IOSCO Principles for FMIs (PFMI) also have a concept of "critical service providers", which encompasses third-party service providers that are essential to an FMI's operations such as IT and messaging providers.[41] Annex F of these principles sets out expectations aimed directly at critical service providers (in contrast with most other documents, which are directed principally at FIs). The Eurosystem, for instance, implements consistent with the PFMIs an oversight policy that focuses on critical service providers of systemically important payment systems in the euro area.

Moreover, certain authorities including across the EU, the MAS and the PRA expect banks to have sound risk management practices to manage risks arising from all "third-party arrangements" even if these arrangements do not fall within the definition of "outsourcing" and are not covered by specific requirements.

2. Intra-group outsourcing

Most surveyed authorities do not differentiate outsourcing or third-party services provided by an institution that is part of a FI's group (intra-group) versus those provided by external (third-party) service providers. There is, however, a widespread recognition that some requirements on outsourcing or third-party risk management can be met in way that takes into account both the particular risks and efficiencies in intra-group situations. For example, the Bank of Italy takes into account that "a group can be deemed as a single economic entity" and "the power of direction and coordination of the parent undertaking" in intra-group situations.

In the EU, MiFID II, the MiFID Commission Delegated Regulation (art. 31.4) (for investment firms), and the recent EBA *Guidelines on outsourcing arrangements* for banks, investment firms, payment institutions and e-money institutions state that, if a FI in scope and its service provider are members of the same group, the institution may (in complying with certain requirements and expectations on outsourcing) take into account the extent to which it "controls the service provider or has the ability to influence its actions".[42]

The EBA guidelines further clarify that "intragroup outsourcing is subject to the same regulatory framework as outsourcing to service providers outside the group. Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the group". However, "the notion of proportionality will be taken into account in intra-group outsourcing arrangements (see Guideline number 47). In the UK, Financial Conduct Authority (FCA) has rules and guidance in their Handbook relevant to intra-group outsourcing, such as operational risk management.[43]

---

41 CPMI-IOSCO (2012)

42 EBA (2019a)

43 https://www.handbook.fca.org.uk/handbook/SYSC/8/

Meanwhile, the Eurosystem with respect to FMI oversight does not consider an intra-group relationship as a third-party relationship (i.e. critical service provider relationship) but rather focuses only on external, contractual providers.

IOSCO's proposed updates to its *Principles on Outsourcing* include a balanced articulation of the relative benefits and risks of intra-group outsourcing, which they note "may be different to those encountered in outsourcing to an unaffiliated external service provider".[44] In particular, the regulated entity may have the ability to control or influence the actions of the affiliated service provider, and the regulated entity may be more familiar with the affiliated service provider's business attributes. These factors might reduce certain risks involved in outsourcing compared to outsourcing to an unaffiliated service provider". Conversely, intra-group outsourcing may potentially increase risk in certain instances: for example, the relationship may be a less than arms-length, and the regulated entity and its clients may have different interests from those of the affiliated service provider".

3. Governance and risk management

Requirements and regulatory/supervisory expectations on governance and risk management in relation to outsourcing and third-party relationships are remarkably consistent across surveyed authorities. Common themes include:

- *The ultimate responsibility of the board for overseeing the effective management of all risks, including outsourcing and third-party risks.* There is a corresponding need for appropriate board skills and effective board engagement.

- *The importance of clear roles and responsibilities within the outsourcing framework*. This may be achieved by establishing multi-disciplinary teams, for example, as expected by MAS or making a director or senior employee accountable for the FI's outsourcing framework, for example, as required by the UK's Senior Managers and Certification Regime.

- *The importance of establishing a responsible unit for the monitoring and control of each outsourced function or service, and a proper reporting to the board and management.*

- *The integration of a FI's third-party risk management process with its enterprise-wide risk management framework and the proper involvement of the three lines of defence*[45] or *an internal risk management and control model to ensure appropriate segregation duties*.

---

44 IOSCO (2020)

45 This note uses the BCBS's definition of the three lines of defence, which comprises a business line (first line); a risk management function and a compliance function independent from the first line of defence (second line); and an internal audit function (third line) independent from the first and second lines. See BCBS (2015) *Corporate Governance Principles for Banks*, 8 July.

- *The requirement for a policy on outsourcing and third-party risk management, which should be approved and periodically reviewed by the board.* For instance, the Bank of Spain requires review at least bi-annually.

- *The need for an effective risk management framework for outsourcing and third-party arrangements.* In some jurisdictions, such as Brazil or Turkey, this can be a component of FIs' broader information security or operational risk management frameworks.

- *The importance of carrying out a comprehensive risks analysis prior to proceeding with the outsourcing process.*

- *The need to conduct appropriate due diligence in the selection of the third-party service provider to ensure that it has the ability, capacity and any authorisation required by law* to deliver the required functions or activities in a satisfactory manner, taking into account the undertaking's objectives and needs.

- *The need to inform the supervisor about material outsourcing arrangements*. Some supervisory authorities require an ex-ante notification (e.g. Hong Kong, Spain), while others require ex-post notification (e.g. Brazil, Korea). Prior notification of the outsourcing of critical operational functions is mandatory in all EU Member States for insurance and reinsurance undertakings. [46] A number of jurisdictions require authorisation from the supervisory authority prior to entering into arrangements to outsource activities outside their jurisdiction, and inform them if the activity is performed inside their own jurisdiction (e.g. Australia and Mexico).

4. Data security, information and cyber security requirements

Requirements relating to data, information and cyber security are becoming increasingly common.

- Some supervisory authorities, such as BCB, have included requirements and expectations on the security of data shared with third parties (including those located outside their jurisdiction) as part of detailed regulation on cyber-risk.

- Some other supervisory authorities have included provisions on data security in their regulation of outsourcing or third-party risk management.

- Other supervisory authorities have done both. For instance, the EBA *Guidelines on outsourcing arrangements* [47] and the EIOPA *Guidelines on outsourcing to cloud service providers* [48] include expectations on data security. Likewise, the EBA *Guidelines on Information and Communications Technology Risk (ICT) Management* [49]

---

46 See DIRECTIVE 2009/138/EC.
47 See EBA (2019a).
48 See EIOPA (2020).
49 See EBA (2019b).

and the EIOPA *Guidelines on Information and Communication Technology (ICT) security and governance*,[50] include expectations on how FIs should manage ICT risks, including data security, in their interactions with third parties. The MAS has also included provisions on data security in their *Guidelines on outsourcing*, in addition to regulations on technology risk management that require FIs to implement IT controls to protect customer information regardless of whether the information resides with third parties.[51]

- Several authorities, such as those in Brazil, Hong Kong, the EU and the US have also highlighted the data security requirements established by personal data protection legislation.

Across surveyed jurisdictions, regulatory requirements on data, information and cyber security tend to cover certain common areas, such as the followings:

- *Data location*: All surveyed authorities require FIs to manage the risks relating to the routing, storage or transfer of data across jurisdictions.

  - Several authorities, such as those in Brazil, the EU and UK expect FIs to take a risk-based approach to data location and implement adequate controls. This risk-based approach should balance:

    - potential legal risks, conflicting legal or regulatory requirements and challenges to firms' and supervisory or resolution authorities' ability to access data in certain overseas jurisdictions (including any jurisdictions through which data may be routed) due to local law enforcement, legal or political circumstances; and

    - the potential operational resilience benefits of outsourced data being stored in multiple locations.

  - Other supervisory authorities, such as CMBT in Turkey, allow the sharing of data with third parties located overseas but require FIs' "primary systems" (i.e. the hardware, software and data enabling the secure and electronic access of the information required for the fulfilment of the FI's legal and regulatory obligations) to be located domestically. Similarly, in Korea, FIs that process personal information are required to have domestic computing facilities.

  - Some authorities including authorities that did not take part in the survey require outsourced data to remain in the same jurisdiction as the FI. Such data localisation policies may pose additional risks for firms and authorities, and limit the potential enhancements to FIs' resilience of certain outsourcing and third-party arrangements (e.g. cloud service providers).

---

50 EIOPA (2020) *Guidelines on information and communication technology (ICT) security and governance*, 12 October

51 MAS (2018) *Guidelines on outsourcing*, 5 October

- *Data access*: Irrespective of location, most authorities have issued requirements or guidance for FIs to ensure that contractual arrangements with third parties enable them and the FIs to access FIs' data held by third parties, including those used in stressed scenarios (e.g. the insolvency of the service provider or the resolution of the FI);

- *Data classification and protection*: Responsibility for the classification of data tends to remain with FIs in practically all outsourcing and third-party arrangements. FIs also commonly remain responsible for ensuring that there are appropriate measures to protect these data, such as encryption and access management. A few authorities (e.g. BCB, MAS) require or expect FIs to ensure that data shared with third parties is promptly removed from the third parties' possession, deleted, destroyed or rendered unusable in the event that the outsourcing or third-party arrangement is terminated.

- *Data breach reporting*: Several authorities expect outsourcing agreements to address the obligation of third parties to inform FIs of any breach of security or confidentiality of outsourced data.

5. Supply chain management

In general, most surveyed authorities expect FIs to retain responsibility, and manage risks relating to the sub-contracting of services provided by third parties (known as sub-outsourcing, chain outsourcing or supply chain management), which can involve fourth parties, fifth parties and beyond. In some cases, there may be up to twenty providers involved in an outsourcing chain.

There is a general recognition that, the longer and more complex a chain of service providers is, the more challenging it becomes for FIs and supervisory authorities to manage the relevant risks or even to identify all the different providers involved. FIs should generally have the ability to contractually limit, approve, or object to at least some forms of sub-contracting; be notified of material changes to sub-contractors; and have the opportunity to terminate arrangements in certain circumstances. Some supervisory authorities, such as the South African Reserve Bank (SARB), establish that the agreements for material business activities or functions should include clauses so that any subcontracting by a third-party service provider will be the responsibility of the third-party service provider.

Most supervisory authorities expect that institutions ensure that contractual rights for FIs and the relevant authorities remain throughout the supply chain (e.g. access and audit rights).

6. Access, audit and information rights

Ensuring that written agreements between FIs and third parties give institutions and authorities effective rights to access, audit and obtain information from third parties is an important and sometimes contentious issue.

Most surveyed authorities expect written agreements, or at least those relating to critical or important functions or services to give them and FIs all necessary rights to ensure that the third-party service provider is delivering the relevant function or service in line with applicable

legal and regulatory requirements, the FI's risk tolerance, and contractually agreed performance and risk indicators.

For instance, in the EU, the EBA *Guidelines on Outsourcing Arrangements* provide that all arrangements relating to the outsourcing of critical or important functions should ensure that service providers grant to FIs in scope, supervisory authorities, resolution authorities (if different) and persons appointed by the above "full access to all relevant business premises (e.g. head offices and operation centres) including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors".[52] Similarly, Article 38 of the Solvency II Directive requires service providers to cooperate with supervisory authorities of insurance and reinsurance undertakings in connection with an outsourced activity, including by providing supervisory authorities with effective access to data related to the outsourced activity. Article 38 of the Solvency II Directive also empowers the EU Member State where the service provider is located to permit the supervisory authorities of an insurance or reinsurance undertaking to carry out on-site inspections (directly or through intermediaries) at the premises of the service provider.[53]

Most authorities do not specify in detail how FIs should negotiate and exercise their contractual access, audit and information rights. However, some jurisdictions (e.g. Mexico) require FIs to have policies and procedures enabling them to audit the infrastructure, controls and operation of third-party data centres twice a year, along with requirements to report the results of these audits to their boards of directors.

A common challenge (linked to the issue of supply chain management in Section 5 of Annex) is whether FIs' access, audit and information rights should extend to (at least material) sub-contractors of the original service provider. In some jurisdictions, such as Japan, a FI is recommended to consider whether its outsourcing contract relating to important services set out explicitly that the FI have the right to audit the subcontractor.

In some jurisdictions supervisory authorities' ability to access, audit and obtain information from certain third parties is to some extent, guaranteed by law. However, even in those jurisdictions, there are still requirements or expectation on FIs to contractually secure "accurate and timely" access, audit and information rights.

- In the US, such an authority is limited to the specific service, and does not extend supervisory or regulatory authority over the service provider itself. It is also only applicable to the banking sector and in certain segments of the insurance sector.

- The BoE/PRA also has a far-reaching statutory power to gather information it deems relevant to financial stability, which can apply to service providers (as defined in Financial Services and Markets Act) subject to certain conditions.

In addition to "traditional" audits of outsourcing or third-party service providers' premises, alternative or complementary audit methods have emerged in recent years in light of the growth

---

52 See EBA (2019a).

53 See DIRECTIVE 2009/138/EC.

of technology third-party service providers. Authorities are increasingly recognising the merit of these alternative audit methods as they can be less disruptive to service providers running multi-tenant environments, such as cloud service providers, as well as enabling FIs to share costs and expertise. For example, in the UK, the PRA acknowledges the importance of FIs exercising their access, audit and information rights in an outcomes-focused manner. To enable this, the PRA recognises various methods such as those set out below, which may enable FIs to meet their regulatory obligations subject to certain conditions.

- *Certificates and reports facilitated by outsourced service providers (known as "third-party certification") if appropriately reviewed by the FI.* Most supervisory authorities recognise the potential use of certificates and reports supplied by third-party service providers and produced in accordance with internationally recognised standards (e.g. ISO, NIST, Cloud Security Alliance (CSA)) as a potential, at least partial, means for service providers to provide FIs with some level of assurance.

- *Audits organised by groups of FIs sharing one or more service providers and performed by representatives of the participating firms or* specialists *appointed on their behalf ("pooled audits")*.

Some jurisdictions explicitly set out what steps FIs should take following an audit of a third-party service provider. For instance, in Hong Kong and the US, in certain sectors, FIs are expected to establish action plans of remedial measures required.

7. Concentration risk considerations

Many authorities monitor concentration risk of third-party service providers at the financial system-wide level. It is possible that a small number of dominant third-party service providers to FIs, depending on the criticality and substitutability of the services being provided, could become single points of failure thereby giving rise to financial stability risks (see also Section 3 of the main note).

Compared to the micro-prudential regulatory requirements, expectations and supervisory practices on outsourcing and third-party risk management set out in the previous sections, the identification, mapping, monitoring and oversight of third parties that might be significant to the financial system by authorities is consistently less developed across surveyed jurisdictions. Data are often lacking, incomplete or only available from commercial data providers.[54]

7.1. Identification and mapping

There is a growing awareness of the importance of identifying and mapping those third parties whose disruption or failure could impact FIs or, potentially, financial stability and improve their understanding of third-party interconnectedness in the financial system. This is in turn giving rise to a number of regulatory and supervisory initiatives. Followings are some examples:

[54] In some cases, authorities have purchased data from surveys of FIs from such data providers. See FSB (2019).

- Resolution 4658 requires FIs in Brazil, to communicate the contracting of relevant cloud computing, data processing and storage services to the BCB. The communication includes the identity of the service provider, the type of service and the location of relevant data. This gives the BCB a database of IT services and service providers, with useful information to map sector-wide dependencies and monitor the location of FIs' data. Likewise, Circular 3909 establishes the same regulatory requirements for payment institutions in Brazil.[55]

- Some authorities, for instance those in the EU, require FIs to notify them or obtain approval for critical (or important) outsourcing or third-party arrangements. These authorities could pool firms' notifications to try and identify the key service providers of material outsourcing and third-party services.

- Some authorities collect data from FIs that could help them form a partial picture of those third parties with the potential significance to the financial system. For instance, as part of current or proposed initiatives to strengthen FIs' operational continuity in resolution (OCIR) or operational resilience.

- Finally, some authorities carry out ad hoc data collection exercises where they ask FIs to identify their most important service providers.

An emerging trend is the use of standardised inventories or registers of service providers by some supervisory authorities. For example, EU banks are expected to maintain a register of all their cloud outsourcing arrangements and make it (or parts thereof) available to supervisory authorities upon request. The EU's Single Resolution Board (SRB) expects banks to develop and maintain an up-to-date searchable database ("service catalogue") in which mapped information is gathered and can be accessed reliably, including in a stressed situation, for resolution planning or execution purposes. [56] Likewise, from 31 December 2021, EU banks will be expected to maintain a register of all their outsourcing arrangements (EBA Outsourcing Register). The MAS *Guidelines on Outsourcing* expect FIs in Singapore to maintain a similar register.[57]

Inventories and registers can be a valuable tool to identify and monitor concentration risks, including on a cross-border basis. Certain conditions will increase the utility of such tools and make it more likely they will fulfil their potential. First, when FIs fill in the requisite information consistently, results can be better pooled and analysed. This can be a challenge given that a lot of information on outsourcing and third-party arrangements is qualitative. Second, the information can be better used when authorities have mechanisms and tools to collect, aggregate and compare the information provided by FIs. To make mapping most effective, authorities would need to develop criteria and methodologies to understand the nature of services and how essential they are. Cross-border dialogue would be helpful to identify potential dependencies that may occur across borders.

---

55 In the Brazilian financial regulatory framework, a "Resolution" is a regulation issued by the National Monetary Council and applies to the entire financial system whereas a "Circular" is a regulation for entities under BCB's jurisdiction.

56 SRB (2020) *Expectations for Banks*, April

57 See MAS (2018).

7.2. Mitigants and exit strategy

Given concerns about the lack of substitutability of certain third-party services, there is a growing focus on FIs to develop and test robust business continuity plans and exit strategies for third parties, as well as adequately manage vendor lock-in and related risks.

A common aim of the supervisory expectations for continuity and resilience is to better enable FIs to withstand and recover from an outage or failure at a third-party service provider without undue disruption to the provision of the most important services they provide to the economy.

Additionally, many authorities have issued supervisory guidance addressing vendor lock in and concentration risks through exit planning. If necessary, this may require FIs to exit a given outsourcing or third-party agreement and move the relevant function, service or data to an alternative service provider, back in-house or seek alternative methods to ensure the continued provision of the service. Some authorities, like the BCB, also require that contractual arrangements between a FI and a third-party service provider cover the deletion of FI's data by the third-party service provider following completion of the exit plan.

Most jurisdictions address business continuity planning and exit strategies either as part of their regulation of outsourcing and third-party risk management and/or in separate, complementary requirements on business continuity management that extend to FIs' third-party relationships, as is the case in Singapore. Some jurisdictions, such as Argentina, are also planning to address exit strategies as part of upcoming supervisory guidelines on IT management.

Developing and executing exit strategies can be challenging in practice in the case of certain intra-group arrangements. Some jurisdictions (e.g. Germany) allow the establishment of specific processes to "be waived in the case of outsourcings within a group or within a network of affiliated FIs" on proportionality grounds.[58]

Some supervisory authorities, such as some authorities in the US, make clear that these contingency plans, exit strategies and substitutability assessments should be established in the early stages of an arrangement (i.e. during the due diligence phase).

Similarly, in the specific case of material cloud outsourcing arrangements, the PRA expects firms in the UK it regulates to assess the resilience requirements of the outsourced service and data and determine which of the available cloud resiliency options is most appropriate. These may include multiple availability zones, regions or service providers.

[58] See Kelp T (2019) *One for many*, 26 August (available on BaFin website).