FSB FINANCIAL STABILITY BOARD

Enhancing Third-Party Risk Management and Oversight

A toolkit for financial institutions and financial authorities

4 December 2023

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

Table of Contents

Executive summary

Financial institutions rely on third-party service providers for a range of services, some of which support their critical operations. These dependencies have grown in recent years as part of the digitalisation of the financial services sector and can bring multiple benefits to financial institutions including flexibility, innovation and improved operational resilience. However, if not properly managed, disruption to critical services or service providers could pose risks to financial institutions and, in some cases, financial stability.

The FSB has developed a toolkit for financial authorities and financial institutions as well as service providers for their third-party risk management and oversight. The toolkit also aims to reduce fragmentation in regulatory and supervisory approaches across jurisdictions and different areas of the financial services sector, thereby helping mitigate compliance costs for both financial institutions and third-party service providers, and facilitate coordination among relevant stakeholders.

The toolkit comprises 4 main chapters. Chapter 1 presents a list of common terms and definitions as a foundation. While complete harmonisation of terms is not always possible or desirable, a common understanding of terms and definitions can help improve clarity and consistency, assisting and enhancing communication among stakeholders under interoperable approaches.

Chapter 2 summarises the toolkit's approach. In particular, the primary emphasis is on critical services given the potential impact of their disruption on financial institutions' critical operations and financial stability. It also looks holistically at third-party risk management, which is wider than the historical narrower focus on outsourcing, in light of changing industry practices and recent regulatory and supervisory approaches to operational resilience. Similar to the terms and definitions, the toolkit aims to promote interoperability of regulatory and supervisory approaches, stopping short of full homogeneity. Finally, the principle of proportionality is applicable throughout the toolkit, which allows the tools to be adapted to smaller, less complex institutions or intra-group third-party service relationships.

Chapter 3 sets out tools to help financial institutions identify critical services and manage potential risks throughout the lifecycle of a third-party service relationship. These tools seek to help financial institutions to:

- Identify critical services consistently yet flexibly;
- Have consistent mapping of financial institutions' third-party service relationships;
- Conduct due diligence, contracting and ongoing monitoring of critical services and service providers;
- Be informed of incidents affecting critical services in a timely way;
- Manage risks relating to their third-party service providers' use of service supply chains;
- Implement and test business continuity plans and coordinate with their third-party service providers for their business continuity;

- Develop effective exit strategies; and
- Strengthen the identification and management of service provider concentration, and concentration-related risks.

Chapter 4 sets out financial authorities' current and developing approaches and tools for supervising how financial institutions manage third-party risks, and for identifying, monitoring and managing systemic third-party dependencies and potential systemic risks. In some jurisdictions or regions, financial authorities have or are in the process of acquiring regulatory powers to formally designate certain service providers as critical for the financial system and oversee these service providers and their services to financial institutions. However, this is not the case in other jurisdictions. Accordingly, the tools in this toolkit are versatile and can be adopted through either voluntary collaboration between financial authorities, financial institutions and relevant service providers, requirements or expectations on financial institutions, or direct requirements or expectations on service providers.

Among other areas, the tools cover:

- Incident reporting to financial authorities, including the possibility of enhancing the existing cyber reporting framework to include reporting by service providers where an incident could give rise to potential risks to financial stability;
- Non-exhaustive criteria to help financial authorities identify systemic third-party dependencies and assess potential systemic risks; and
- Tools to identify and manage potential systemic risks, including but not limited to sector-wide exercises and incident response coordination frameworks.

Finally, the importance of cross-border supervisory cooperation and information sharing is underscored. For this objective, the chapter sets out certain ways to explore greater convergence of regulatory and supervisory frameworks around systemic third-party dependencies, options for greater cross-border information-sharing, and cross-border resilience testing and exercises.

Introduction

Financial institutions have long relied on outsourcing and other third-party service relationships. However, in recent years, the extent and nature of financial institutions' interactions with a broad and diverse ecosystem of third-party service providers have evolved and increased. These developments have brought both benefits and the introduction of different types of risks to financial institutions. If they are not appropriately managed, these relationships could lead to risks to financial stability.

Against this backdrop, in November 2020 the Financial Stability Board (FSB) published a discussion paper on regulatory and supervisory issues relating to outsourcing and third-party service relationships. As part of the consultation process, in February 2021 the FSB held an outreach meeting, which was attended by a wide range of external stakeholders.[1]

Based on feedback to the discussion paper, in September 2021 the FSB's Standing Committee on Supervisory and Regulatory Cooperation (SRC) decided to develop a toolkit for financial regulatory and supervisory authorities (hereafter "financial authorities") focused on their oversight of financial institutions' reliance on critical service providers, including common terms and definitions on third-party risk management.[2]

The objectives of the toolkit are to (i) reduce fragmentation in regulatory and supervisory approaches to financial institutions' third-party risk management across jurisdictions and different areas of the financial services sector; (ii) strengthen financial institutions' ability to manage third-party risks and financial authorities' ability to monitor and strengthen the resilience of the financial system; and (iii) facilitate coordination among relevant stakeholders (i.e. financial authorities, financial institutions and third-party service providers). The work could also help mitigate compliance costs for both financial institutions and third-party service providers.

To this end, the FSB has prepared this document. The document leverages the insights of members of a Workstream on Third-Party Risk and Outsourcing under the SRC and inputs from external stakeholders. It is also informed by a survey on practices and challenges, as well as financial authorities' expectations in relation to financial institutions' third-party risk management.[3]

Recognising differences across jurisdictions and financial institutions, the document proposes a flexible and risk-based set of tools ("toolkit") which financial authorities and financial institutions may consider based on their circumstances, including the legal framework and specific features of the financial services sector in their jurisdictions. At the same time, the toolkit seeks to promote comparable and interoperable approaches across jurisdictions. The toolkit is designed to complement and build on relevant existing standards and guidance by international Standard-Setting Bodies (SSBs) and financial authorities, but not replace them.

---

1 See FSB (2020), *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper*, November, and FSB (2021), *Outsourcing and third-party risk – Overview of responses to the public consultation*, June.

2 See FSB (2022), *FSB Work Programme for 2022*, March and also FSB (2023) *FSB Work Programme for 2023*, March.

3 The survey was conducted in mid-2022 and received 24 responses from financial authorities, including standard-setting bodies, and 17 responses from external stakeholders, including industry associations.

1. Common terms and definitions

This chapter presents a list of common terms and definitions as a foundation for the subsequent sections of the document. Common understanding of terms and definitions can improve clarity and consistency regarding third-party risk management across financial institutions, assist financial authorities with regulatory cooperation, improve communication with third-party service providers, and promote interoperable approaches that make oversight and risk management more efficient for financial institutions, financial authorities and third-party service providers.

Due to differences in regulation and industry practices across jurisdictions, and in the existing definitions used by different SSBs, complete harmonisation of terms is not always possible or desirable. A pragmatic approach is therefore required. The list of terms is not intended to be exhaustive and is limited to those that are necessary and relevant to the document.[4] It is based primarily on feedback from industry and financial authorities. To ensure consistency and transparency, the list of terms was assessed against a set of criteria, which are similar to those used in the FSB Cyber Lexicon but adapted to third-party risk management:[5]

- Criterion 1 (objectives): The terms should be useful for: developing a common understanding across the financial services sector (and with third-party service providers); assessing and monitoring financial stability risks; sharing information across financial authorities; and guiding the work of the FSB and/or other SSBs.
- Criterion 2 (scope): The focus should be on core terms that are relevant to third-party risk management in the financial sector.
- Criterion 3 (exclusion of excessively technical terms): Terms that are too technical for the relevant policy context should be excluded.
- Criterion 4 (exclusion of general terms): General terms that are used by financial authorities and financial institutions in areas extending beyond third-party risk management should be excluded.

Based on the approach described above, the following terms have been selected and defined, with the aim to keep the definitions simple and clear.[6]

- **Third-party service relationship**:[7] A formal arrangement for the provision of one or more services, or parts thereof, to a financial institution by a service provider. For the purposes of the toolkit:
  - Services include but are not limited to activities, functions, processes and tasks;

---

4 Some of the terms are used in other third-party risk and outsourcing frameworks (e.g. international frameworks as listed in Annex 1 and national frameworks) in a different way. Therefore, care should be exercised in cross referring to these terms.

5 See FSB (2018), *Cyber Lexicon*, November.

6 Some terms and definitions refer to each other. They should be considered as one set of terms and definitions.

7 Third-party service relationship may be referred to as third-party service dependency or third-party service arrangement.

- Third-party service relationships include arrangements for the provision of services to a financial institution by an intra-group service provider; and

- Third-party service relationships exclude financial services transactions between financial institutions and their employees, customers or counterparties (e.g. taking deposits from or lending to consumers; providing insurance to policyholders; or providing/receiving financial market infrastructure (FMI) services, such as clearing or settlement, to other financial institutions), but include services supporting these functions (e.g. compliance or back-office activities relating to these transactions).

- **Service provider**: An entity or individual that provides services to one or more financial institution either directly or indirectly (e.g. as part of the supply chain of another service provider). There are several types of service providers.[8]

  - **Third-party service provider**: A service provider that provides services to one or more financial institutions under a third-party service relationship.

  - **Nth-party service provider**:[9] A service provider that is part of a third-party service provider's supply chain and supports the ultimate delivery of services to one or more financial institutions.

  - **Intra-group service provider**: A service provider that is part of a financial institution's group and provides services predominantly to entities within the same group. Intra-group service providers may include a financial institution's parent undertaking, sister companies, subsidiaries, service companies or other entities that are under common ownership or control.[10]

- **Outsourcing**: A category of third-party service relationships where a financial institution uses a service provider to perform, on a recurrent or an ongoing basis, services, or parts thereof, that would otherwise be undertaken, or could reasonably be undertaken, by the financial institution itself.

- **Supply chain**: The network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a financial institution. For the purposes of the toolkit, the scope of supply chain is limited to the services under a third-party service relationship.

---

8 Service providers consist of third-party service providers and nth-party service providers. Intra-group service providers could be either third-party service providers or nth-party service providers.

9 Nth-party service providers may be referred to as sub-contractors, sub-outsourced service providers or indirect service providers. A fourth-party service provider provides services to one or more third-party service providers, and this concept can be further extended into nth-party service providers.

10 Branches are not considered intra-group providers, as they are not separate legal entities from their head offices. However, the provision of services from a head office of a financial institution to its overseas branches, or between branches, is not riskless. Therefore, in practice a proportionate risk-based approach to risk management and oversight of head office/branch relationships may be appropriate as further discussed in section 2.4.

- **Critical service**: [11] A service provided to a financial institution whose failure or disruption could significantly impair a financial institution's viability, critical operations,[12] or its ability to meet key legal and regulatory obligations.

- **Critical service provider**: A service provider that provides critical services to a financial institution.

- **Systemic third-party dependency**:[13] A dependency on one or more services provided by a service provider to financial institutions where their disruption or failure has been identified by a relevant financial authority as having potential implications for financial stability.

2. Scope and general approaches

This chapter summarises the approach taken by this document to a number of cross-cutting issues. Section 2.1 discusses the focus on "critical services" (as defined in Chapter 1). Section 2.2 clarifies the document's holistic approach to financial institutions' management and financial authorities' oversight of third-party service relationships, as opposed to a subset thereof, such as "outsourcing", which has historically been the focus of regulatory and supervisory frameworks. Section 2.3 discusses the desirability of approaches that promote interoperable cross-border regulatory and supervisory practices to third-party risk management. Section 2.4 considers the application of the principle of proportionality in the context of third-party risk management. It discusses how regulatory expectations can differ based upon several factors, including the business model, complexity, function, internal organisation, risk profile, scale and size of different financial institutions, and availability of back-up capacities.

The toolkit is intended to be used by both:

- Financial institutions in their management of third-party risks; and

- Financial authorities as they consider their approaches to the oversight of financial institutions' third-party service relationships (in particular, those involving critical services), and the identification, monitoring and management of systemic third-party dependencies and potential systemic risks.

In line with the approach set out in Chapter 1, for the purposes of the toolkit, regulated financial institutions[14], to the extent they are engaging in financial services transactions, such as

---

11 Financial authorities in some jurisdictions use terms such as "material services" and "important services" in a synonymous way. However, such concepts are often used to qualify services of a financial institution to their customers. This report focuses on the critical services provided to financial institutions by service providers that are all or in part provided by a service provider.

12 In the toolkit, the term "critical operations" has the same meaning as in BCBS (2021), *Principles for Operational Resilience*, March, i.e., "activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of the [financial institution] or its role in the financial system". The term "critical operations" includes but is not necessarily limited to "critical functions" as defined in FSB (2016), *Guidance on Arrangements to Support Operational Continuity in Resolution*, August.

13 Financial authorities in some jurisdictions may use a different term in a similar context, taking into account the different approaches used in the jurisdictions (see an introductory paragraph of Chapter 4 and Section 4.3.1).

14 This exclusion also applies to services provided by FMIs within the scope of the CPMI-IOSCO Principles for Financial Market Infrastructures and to financial messaging infrastructure and market data or information services subject to oversight by financial authorities.

correspondent banking, lending, deposit-taking, provision of insurance, clearing and settlement, and custody services, are generally not considered third-party service providers, and the financial services they provide are not in the scope of third-party service relationships. While these financial services might be objectively critical for any financial institutions that rely on them, the risks they raise are addressed through other, often more specific financial regulatory and supervisory frameworks.

This document aims to complement and build upon the existing work of international standard-setting bodies (SSBs) (i.e. Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI), International Organization of Securities Commissions (IOSCO), International Association of Insurance Supervisors (IAIS)) and other international organisations (e.g. the G7), which have developed, and in some cases recently updated, international standards and guidance addressing third-party risk management in the financial sector (see Annex 1). Financial authorities and financial institutions rely on these standards and guidance, which may be specific to particular areas of the financial services sector (e.g. banking, insurance). The toolkit in this report is not designed to duplicate these existing international standards and guidance, but to complement and enhance their effectiveness by promoting greater regulatory and supervisory interoperability across jurisdictions and among different areas of the financial services sector.

2.1. Focus on critical services

The toolkit focuses primarily on "critical services" (as defined in Chapter 1) as these are the services whose disruption or failure could impair individual financial institutions' viability, critical operations and/or ability to meet key legal and regulatory obligations.[15] However, this focus on critical services does not suggest that third-party service relationships involving the provision of non-critical services to financial institutions do not warrant appropriate and proportionate risk management.

While the primary focus of the toolkit is on critical services, certain sections of the toolkit consider non-critical service relationships, where appropriate. In particular, this is the case in the sections on registers of third-party service relationships (Section 3.4), financial institutions' management of concentration risks (Section 3.8) and the identification of systemic third-party dependencies (Section 4.3).

Many of the concepts discussed in the toolkit, including criticality, are dynamic and can vary over time depending on the circumstances and context. For instance:

- The criticality of a service to a financial institution can vary over time based on the financial institution's reliance on that service and changes in its relationship with the service provider.

[15] In the toolkit, "key legal and regulatory obligations" refer to those legal and regulatory obligations that a financial institution needs to maintain full and timely compliance even in the event of a severe disruption of a critical service. Which legal and regulatory obligations are key will vary by jurisdiction and depend on factors such as a financial institution's business model and size and the consequences of, and remedies available for, partial or temporary non-compliance.

- At any given point, a service may be critical to one financial institution but not to another due to differences in their respective business operations and use of the service. Criticality may depend on how a service is used within differing business models, including the financial institution's complexity, risk profiles, service volume, as well as the availability of back-up or substitute providers for the service.

As discussed in Chapter 4, where one or a limited number of service providers provide critical services to many financial institutions and a quick, seamless transition to an alternative provider in case of disruption would be impractical, impossible or unduly risky, financial authorities may conclude that these services and service providers give rise to a systemic third-party dependency. Where this is the case, financial authorities may place higher expectations on the resilience of the relevant services and seek additional assurance from the service providers given their importance to financial stability.

2.2. Holistic focus on third-party risk management

Financial regulation has traditionally focused on financial institutions' outsourcing relationships. However, in recent years, the types of activities or functions that financial institutions would typically perform in-house have changed. As a result, financial institutions have become increasingly reliant on third-party service providers for services that they had not previously undertaken. Additionally, financial authorities' increasing focus on operational resilience has led to requirements and expectations on financial institutions to effectively manage the risks in all their third-party service relationships, not just outsourcing, given the criticality of some non-outsourcing, third-party services to the continued operations of financial institutions.[16] The deterioration, disruption or failure of critical services or the service providers that provide them may pose risks to financial institutions and, in some instances, to financial stability (see Chapter 4).

Accordingly, in line with recent regulatory frameworks on operational resilience[17] and technology risk management by financial authorities and SSBs,[18] the toolkit takes a holistic, risk-based approach to third-party risk management, which continues to include but is not limited to outsourcing.

A central tenet of this holistic, risk-based focus on third-party risk management is to promote a consistent regulatory approach leading to an effective but proportionate assessment of all third-party service relationships involving the provision of critical services to financial institutions. This approach includes the delivery of a critical service to financial institutions directly by a third-party

---

16 The examples of broader third-party services that do not fall within the definition of traditional outsourcing include data brokers who collate market data or data from social media or in-app device activity and machine learning libraries developed by third parties. Broader third-party service relationships include such arrangements as payment service providers accessing banking functions on behalf of the customers, joint business arrangements such as joint operation of shared data centres, pooled audit of commonly critical third-parties, strategic alliances and industry group for sharing knowledge such as cyber intelligence. Some of those broader third-party service relationships may also be critical to the financial institutions' business operations and financial stability.

17 The toolkit uses the definition of "operational resilience" in the BCBS 'Principles for Operational Resilience' (2021), i.e. "the ability of a [financial institution] to deliver critical operations through disruption. This ability enables a financial institution to protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption.

18 This holistic focus on third-party risk responds to a trend towards commoditisation of business processes and related services. This trend is occurring partly because of technological advancements, which provide both cost efficiency and enhanced quality.

service provider, but also indirectly through that third-party service provider's supply chain (including, if applicable, any nth-party service providers it relies on).

The toolkit also covers critical services to financial institutions provided by intra-group service providers albeit in a proportionate, and risk-based manner detailed below in Section 2.4.

2.3. Regulatory interoperability across jurisdictions and sectors

The toolkit promotes a range of approaches by both financial institutions and financial authorities to achieve common objectives and goals. Promoting comparable, interoperable regulatory and supervisory approaches to third-party risk management across different areas of the financial sector and between jurisdictions can have a number of benefits, including:

- Streamlining the compliance obligations of financial institutions and service providers that operate on a cross-border basis without materially reducing the effectiveness of these obligations; and
- Facilitating coordination among financial authorities, thereby enhancing the effectiveness of national approaches while enabling multiple different regulatory regimes to coexist based on common expectations.[19]

Interoperability of regulatory and supervisory approaches in the financial services sector is particularly important for financial institutions subject to multiple national or regional regulatory and supervisory frameworks. For efficiency and resilience reasons, financial institutions often centralise certain functions (e.g. financial reporting, human resources, cybersecurity) and parts of their infrastructure (e.g. information and communications technology (ICT)) that often rely on third-party service relationships, including for critical services.[20] Limiting the negative consequences of regulatory fragmentation is therefore desirable to achieve strong outcomes across financial institutions.

The same holds true for service providers that provide services across multiple jurisdictions, to multiple areas of the financial services sector, and to sectors outside financial services. Having multiple, fundamentally divergent regulatory and supervisory approaches can create significant challenges to effective and efficient risk management of, and by, service providers.

Interoperability of regulatory and supervisory approaches also allows financial authorities to work more collaboratively and effectively across jurisdictions and different parts of the financial services sector. The potential benefits of greater regulatory and supervisory coordination can arise at multiple points, including when assessing, monitoring, and managing the risk of failure or disruption of critical services with potential cross-border impacts (see Section 4.4).

---

19 Past examples of related areas where regulatory and supervisory interoperability has helped financial institutions and supervisory authorities, include the FSB's toolkit of *Effective Practices for Cyber Incident Response and Recovery; the FSB's Recommendations to Achieve Greater Convergence in Cyber Incident Reporting*; and the 2019 report of IOSCO's *Cyber Task Force on existing frameworks for cyber regulation* (identifying different but comparable core standards or frameworks: the National Institute of Standards and Technology (NIST) Cybersecurity Framework; the 2016 CPMI-IOSCO Guidance on Cyber Resilience; and the International Organization for Standardization (ISO) framework).

20 As discussed in Section 2.4, this centralisation often utilises intra-group services and intra-group service providers.

It is important to note that interoperability does not mean homogeneity. Complete regulatory and supervisory alignment is unlikely to be possible or practical, given legal differences between regimes and the different business models of financial institutions, which mean that risks can differ both between jurisdictions and regions, and across different areas of the financial services sector.[21]

Consequently, regulatory and supervisory interoperability in the context of the toolkit seeks to ensure that individual regulatory and supervisory regimes do not lead to inconsistent requirements and expectations on financial institutions and service providers operating internationally. It does so by setting out aligned and comparable, outcomes-based frameworks to manage third-party risks, while avoiding a one-size-fits-all approach that does not permit differences in regulation or market structure.

2.4. Proportionality

The failure or disruption of a critical service may have a greater impact on financial stability if it affects larger, more complex financial institutions, which may in turn warrant stricter regulatory expectations and more intensive supervision.

Consequently, the FSB developed the toolkit in a way that considers proportionality. Proportionality in the toolkit focuses primarily on how financial institutions' management of third-party risks may vary based on their business model, complexity, cross-border presence, function, risk profile, scale, structure and size. Some of the tools in Chapter 3 may be appropriate for large, complex financial institutions but disproportionate or unsuitable for small, less complex financial institutions. Thus, financial institutions with a smaller operational footprint and fewer resources may be subject to proportionate regulatory expectations in terms of how they manage third-party risks and other operational risks[22], compared to larger or more complex institutions. The principle of proportionality applies to the use of the suggested tools in this report, and to the frequency and intensity of their use.

For instance, smaller, less complex financial institutions may use the auditing and monitoring tools in Section 3 with different frequency and intensity compared to larger, more complex institutions. Proportionality may also be relevant to internationally active financial groups as they may operate businesses of different sizes and complexity globally. In some jurisdictions or markets, a financial institution belonging to a large internationally active financial group may still be small and less complex on an individual entity basis in that local market. The principle of proportionality also applies to service providers depending, for example, on their size and complexity and the risk they pose to financial institutions and financial stability[23]. The tools aimed at service providers are not intended to unduly limit competition or innovation.

---

21 It may often strengthen key goals of operational resilience to have a variety of different but interoperable approaches (e.g. BCBS Principles for Operational Resilience, embracing a principles-based approach to operational resilience).

22 For instance, Article 16 of the EU's Digital Operational Resilience Act (DORA) imposes simplified ICT risk management requirements on certain, in-scope small and non-interconnected financial institutions.

23 The principle of proportionality is embedded in existing SSB standards and national regulatory and supervisory approaches to third-party risk management. For instance, the IOSCO Principles on Outsourcing provide that "the application and implementation of these Principles should be proportional to the size, complexity and risk posed by the outsourcing."

While intra-group services should not be exempt from appropriate risk management, financial institutions and financial authorities can consider risk-based, proportionate approaches to the provision of critical services by intra-group service providers. That is, companies may use effectively their internal group-wide policies and controls to mitigate intragroup arrangement risks. Many financial institutions use intra-group services to provide services in-house, but also to centralise their use of services ultimately provided by a third-party service provider outside the group. For example, instead of each entity in a financial group contracting directly with a third-party service provider for one or more services, a single entity in the group, such as a shared service company, may do so and cascade the relevant service(s) to other group entities through intra-group service relationships (thereby becoming an intra-group service provider to those entities). Intra-group services can be effective in promoting cohesion and resilience within financial groups and are often essential to group-wide risk management. However, intra-group service arrangements are not riskless even if some of the risks they pose may differ from those posed by external third-party service relationships. If not managed appropriately, intra-group services can pose risks for individual financial institutions that are part of a financial group (e.g. major subsidiaries) or the financial group as a whole.[24] The toolkit therefore applies to intra-group relationships proportionately, mindful of these considerations.

This toolkit does not formally include the provision of services from a financial institution's head office to its overseas branches, or between branches, which are sometimes referred to as intra-company. In most jurisdictions, a country branch is not considered to be legally distinct from its overseas head office. Although there are limits to the extent branches can manage risks from any services received from their head offices, local regulations may apply to branches and appropriate risk management should be in place. Some elements of the toolkit may be useful in the case of branches.[25]

Similarly, the provision of financial market infrastructure (FMI) services, such as clearing or settlement from other financial institutions, while important to financial institutions' critical operations, are also excluded from the definition of a 'third-party service relationship' in this toolkit. Consequently financial institutions should take the principle of proportionality into consideration and take appropriate steps to manage the risks in the use of FMI services. This may include the adapted use of certain tools in this toolkit and placing reliance on existing standards and guidance for FMIs when managing the risks they may pose.[26]

---

24 From a risk-based perspective, financial authorities' regulation and supervision should not vary simply because an intra-group service provider provides critical services to a financial institution. However, proportionality may impact on how financial authorities and financial institutions approach, manage and supervise risks in third-party service relationships involving the provision of critical services to a financial institution by an intra-group service provider.

25 For example, in place of a legally binding contract with branches which may not be possible as they are not legally distinct, it may be useful to have a Service Level Agreement to formally document the services required by the branch, the roles and responsibilities of the involved parties including service standards, and the consequences of not meeting these standards. This may be particularly so where the branch needs to meet local regulatory requirements, for instance, with respect to operational resilience for the services it provides locally.

26 The exclusion of these financial services is not intended to imply that financial institutions should not take appropriate steps to manage risk of these transactions, which may include elements presented in the toolkit. Rather, it is intended to avoid unintentional conflicts between the toolkit and more specific expectations applicable to financial services (e.g. expectations on risk management when relying on a central clearing counterparty). In particular, the toolkit is generally not meant to be applied to the use of clearing and settlement and related services from financial market infrastructures, which are subject to their own set of standards and guidance.

3. Financial institutions' third-party risk management

This chapter sets out tools to help financial institutions identify critical services and manage potential risks throughout the lifecycle of a third-party service relationship, which typically includes planning, due diligence and selection of a service provider, contracting, ongoing monitoring, and termination. Regardless of the type of third-party service relationship, the final accountability towards the financial authorities and customers remains with the financial entity and its board and senior management.

Generally, third-party service relationships involving the provision of critical services from service providers should include an assessment of potential benefits and risks and be approved by the board, senior management or an appropriate body of the financial institution.

3.1. Identification of critical services and assessment of criticality

Financial institutions are primarily responsible for and usually best placed to assess the criticality of services they receive or plan to receive.[27] Critical services provided to one financial institution may not necessarily be critical to another. An effective risk-based framework for monitoring and mitigation of risks associated with third-party service relationships benefits from identifying the criticality of services at inception and periodically throughout the service lifecycle. Section 3.1 sets out a range of tools that could help financial institutions identify critical services in a way that balances consistency and flexibility, and can be incorporated into financial institutions' existing policies and practices, as appropriate.

Promoting a common framework for the identification of critical services can promote consistency and comparability and be beneficial to both financial institutions' and financial authorities' objectives of proportionate and effective risk management. It can also facilitate the identification of systemic third-party dependencies by financial authorities. Consistency and comparability can also be beneficial to service providers, providing more predictability in their engagements with different financial institutions.

There are existing elements of international standards and guidance that financial institutions can leverage in their identification of critical services. As noted in Chapter 1, a service is defined as a "critical service", if the failure or disruption of the service would significantly impair the financial institution's viability, its "critical operations" or its ability to meet key legal and regulatory obligations. The concept of "critical shared services" is also relevant and potentially useful.[28]

When identifying critical services and their level of criticality, financial institutions may consider, among other areas:[29]

---

27 As noted in Chapter 4, financial authorities may review financial institutions' risk management of critical services as part of their supervisory and regulatory responsibilities, including review of the identification of critical services.

28 See FSB (2013), *Guidance on Identification of Critical Functions and Critical Shared Services*, July. It defines a "critical shared service" as (i) an activity, function or service performed by either an internal unit, a separate legal entity within the group or an external provider; (ii) an activity, function or service performed for one or more business units or legal entities of the group; (iii) the sudden and disorderly failure or malfunction of which would lead to the collapse of, or present a serious impediment to the performance of critical functions.

29 These areas could also give rise to legal and reputational risks for financial institutions depending on their impact.

- The financial, operational or strategic importance of the service to the financial institution, and any critical operations (including but not limited to critical functions) and core business lines therein that rely on it;

- The level of tolerance for disruption set by the financial institution (or, if applicable, financial authorities or SSBs)[30] regarding the critical operations and core business lines that rely, or will rely, on the service;

- The nature of any data or information shared with the service provider. In particular, whether these data require increased security measures because they are crucial for the financial institution's critical operations, required for regulatory purposes, confidential or sensitive (including but not limited to personal data). Financial institutions may take into account the impact of disruption to the relevant service or service provider on the confidentiality, integrity or availability of these data; and

- The substitutability, or lack thereof, of a service. Services that are easily and readily substitutable may be less critical.

The criticality of a service can vary over time. Services that were originally not critical can become so gradually or upon the occurrence of certain events. Likewise, services that were critical can become less critical, or even become non-critical over time. Financial institutions can assess the criticality of a service prior to entering into a third-party service relationship and reassess it regularly during scheduled review periods, when planning to change their use of the service, and when there is a material change to the service or the service provider (e.g. a corporate reorganisation or transaction, such as merger, that may impact the provision of the relevant service).

3.2. Onboarding and ongoing monitoring of service providers

3.2.1. Due diligence

Financial institutions may conduct appropriate planning and due diligence before entering into a third-party arrangement for a critical service, which can then support financial institutions' subsequent development of appropriate risk monitoring and mitigation measures. In the case of critical services, financial institutions should clearly articulate their expectations for the proposed third-party service relationship (for instance, their expected level of resilience of the critical service) as early as reasonably practicable during the service provider selection process.

The level of due diligence can be applied proportionately to the criticality of the relevant service (see Section 3.1). Tools that financial institutions can leverage as part of their due diligence can include those supporting (i) an analysis of the relative benefits, costs and risks of the proposed arrangement, and an (ii) assessment of the service provider's ability to provide the relevant service. These may include the service provider's:

[30] For instance, the CPMI-IOSCO Principles for FMI note that "An FMI should aim to be able to resume operations within two hours following disruptive events. [An FMI's business continuity plans] should be designed to enable the FMI to complete settlement by the end of the day even in case of extreme circumstances".

- Operational and technical capability and track record, including (if applicable) drawing on any prior engagement between the financial institution and the service provider (in general or in connection with the service to be provided);
- Financial soundness insofar as it can affect the delivery of the relevant services;
- Internal controls and risk management, including its ability to manage ICT, cyber and other operational risks;
- Management of supply chain risks, including use and oversight of nth-party service providers (further discussed in Section 3.5);
- Geographic dependencies and management of related risks. These risks may relate to the economic, financial, political, legal and regulatory environment in the jurisdiction(s) where the relevant service will be provided;
- Key departments and roles involved in the delivery of the relevant service (including key contacts during disruption);
- Potential conflicts of interest;
- Recent or pending relevant complaints, investigations or litigation including (if relevant) at nth-party service providers;
- Ability to deliver the critical service in a way that allows the financial institution to comply with its legal and regulatory obligations;[31]
- Familiarity with the financial services industry and the financial institution's operations;
- Ability to support the financial institution's business strategy and plans (including objectives for innovation where appropriate);
- Business continuity plans, contingency plans, disaster recovery plans and other relevant plans, including, if applicable, recovery time objectives, maximum tolerable downtime and similar concepts. Where possible, these concepts should be consistent or benchmarked to the financial institution's tolerance for disruption in respect of its critical operations; and
- Level of substitutability of the service including:
    - Financial institution's ability (including cost, timing and contractual restrictions) to exit the third-party arrangement and either transition to another service provider or bring the critical service back in-house; and

[31] While the toolkit focuses on financial services regulatory obligations, financial institutions may need to consider broader regulatory obligations as appropriate (e.g. environmental protection, labour, human rights and privacy laws).

- Potential impact of such substitution on the financial institution's critical operations, which may depend on the service provider's ability to provide for an orderly termination.

Although due diligence is linked to pre-contractual activities, financial institutions usually update their due diligence (or parts thereof) as part of their ongoing monitoring of the service provider or within an appropriate period after the commencement of the service (see Section 3.2.3). These updates can be proportionate to the criticality of the service which, as noted in Section 3.1, can change over time. Financial institutions' due diligence should also consider the potential risks of not entering into a given third-party service relationship and balance them against any risks that the third-party service relationship may introduce or amplify. For instance, the risks of not replacing obsolete legacy technology may, in some cases, outweigh the risks that a proposed third-party service relationship designed to replace or update that technology may bring.

3.2.2. Contracting

Legally binding arrangements between the financial institution and a third-party service provider, including clear contractual provisions, can reduce the risks of non-performance, facilitate the resolution of disputes between the financial institution and the service provider about the relevant service, and assist financial authorities in their supervision of the financial institution's third-party risk management.

An arrangement may be signed electronically or on paper and take various forms, including a legally binding contract and a statement of work or an intra-group service agreement, as long as they set out the respective rights and obligations of the financial institution and service provider, including agreed service levels. For simplicity, the toolkit uses the term "contract" as an umbrella term for these arrangements.

The nature and detail of contracts should be appropriate to the financial institution and the criticality of the service. For instance, contracts for the provision of critical services should place greater emphasis on areas such as commitments relating to operational resilience. As part of their toolkit to assess and negotiate contracts for third-party service relationships, financial institutions can consider the following:

- Financial institution's and service provider's respective legal and regulatory obligations, which may include specific provisions or addenda focused on compliance with financial regulatory and supervisory requirements or expectations in the jurisdiction(s) where the financial institution operates;
- Key performance benchmarks, indicators and metrics;
- Conditions governing sub-contracting to nth-party service providers (See Section 3.5);
- Rights for the financial institution to receive accurate, comprehensive and timely information relating to the critical service, including but not limited to incidents (see Sections 3.3 and 4.2) and material changes to the services or service providers;

- Financial institution's right to access, audit and obtain relevant information from the service provider, as appropriate including information on supply chain risk management (see Section 3.5.3), which can extend to financial authorities (see Chapter 4);[32]
- Commitments relating to operational resilience, including business continuity, contingency planning and disaster recovery. These commitments may also comprise minimum service uptime and/or maximum service downtime commitments, recovery time objectives (RTOs) and recovery point objectives (RPOs) (see Section 3.6);
- Costs, including (if applicable) flexibility and scalability based on the financial institution's use of the service;
- Ownership and use of intellectual property (e.g. applications, technology);
- Ownership and transferability of data as well as policies and controls for data access including potential access by other clients;
- Confidentiality of proprietary and strategic information;
- Service provider's obligation to take out insurance against certain risks;
- Right of the financial institution to indemnification in specific circumstances (including any limitations on the service provider's liability);
- Customer complaints handling and dispute resolution mechanisms;
- Choice of law and jurisdiction in case of dispute; and
- Default and termination, including notification period for termination (see Section 3.7).

Financial institutions may exercise these contractual access, audit, and information rights when appropriate. The purpose of these contractual rights is to support financial institutions' identification, assessment, management and mitigation of any risks relating to critical services. The appropriate exercise of these rights can therefore be key to providing the assurance that such an arrangement is being provided as agreed with the service provider and in line with regulatory requirements.

3.2.3. Ongoing monitoring and internal reporting

Ongoing monitoring refers to any continuous or periodic activities performed by a financial institution to assess and manage the risks in a third-party service relationship to the service provider's ability to deliver the service in line with its contractual obligations (taking into account the criticality of the service). Financial institutions may establish a methodology for carrying out their ongoing monitoring, including clear accountability, roles and responsibilities and oversight by an appropriate body. Financial institutions' ongoing monitoring may include:

[32] Financial authorities may be able to obtain these rights indirectly via financial institutions' contracts with service providers, or directly in jurisdictions where they have direct oversight powers over service providers or provision of services (see Chapter 4).

- Key metrics or key performance indicators, associated with a particular service, as appropriate;
- The capability of the service provider to deliver the service in accordance with the terms of the contract, the financial institution's regulatory obligations and its risk appetite and tolerance;
- The financial condition of the service provider and its ability to identify risks to the provider's financial viability; and
- Current and emerging risks, including political and legal environment, that may affect the service provider's ability to deliver a critical service.

Financial institutions may establish processes to evaluate whether risks relating to their third-party service relationships remain within their risk appetite and tolerance for disruption of critical operations and core business lines. To facilitate this, financial institutions may develop and monitor metrics and thresholds relating to the performance and risk of critical services; and establish an escalation process to alert senior management and, as needed, the board if a certain trigger is met or a threshold is being approached. Financial institutions may need to consider how to recruit and retain staff to appropriately manage the risk of novel or complex services that they receive from third-party service providers on an on-going basis.

Financial authorities expect a financial institution to ensure that its contractual arrangements with service providers do not prevent compliance with relevant regulatory requirements and expectations. To do so, a financial institution may seek appropriate contractual rights or other means to assess and obtain ongoing assurance on the design and effectiveness of the relevant control environment for the delivery of critical services.

3.2.4. Possible tools

There are multiple sources of assurance and information that financial institutions and financial authorities can use as tools in their due diligence and ongoing monitoring of service providers (on a risk-based and outcomes-focused approach). These tools may include internationally-recognised certifications or standards.

Internationally recognised certifications or standards can provide assurance about a service provider's controls and help reduce fragmentation of approaches. However, these certifications or standards are often based on checklists of controls and may not, in all cases, provide sufficient assurance to financial institutions or, where applicable, authorities.

Other tools include audit or testing reports by independent parties engaged by either a single financial institution, a collection of financial institutions working collaboratively, financial authorities or the service provider itself. Table 1 includes a non-exhaustive list of other potential tools.

Financial institutions may face challenges performing due diligence and monitoring of services and service providers due to resource and expertise constraints. Collective assurance mechanisms, such as pooled audits may be helpful in these circumstances. Where appropriate

and relevant, financial institutions may also benefit from feedback and relevant insights from financial authorities including on potential risks.

Table 1: Sources and information for assurance

Tools for onboarding and ongoing monitoring
• Information on the service provider's business continuity planning • Documentation on the service provider's controls • Performance-related information (e.g. key performance indicators (KPIs) and scorecards) • Financial condition information such as audited financial reports and credit rating reports • Other relevant information such as data breaches and service disruption reports, risk assessment report on cyber security, details of key nth-party service providers and other components of the service provider's supply chain • Questionnaires (e.g. on cyber-risk and business continuity), which might be standardised or tailored to the service provider • Inspections of the service provider's technology assets and infrastructure (e.g. the premises where the relevant service(s) are provided) • Customised assessments (e.g. assessment of the service provider's cyber and technology vulnerabilities) • Incident reports, root cause analysis and remediation actions completed by independent parties • Technology platforms for the management of workflows associated with the lifecycle of a third-party service relationship and monitoring the financial institution's internal controls

3.3. Incident reporting to financial institutions

Financial institutions are generally required to identify and remediate incidents[33] and may be required to report relevant incidents to financial authorities within a defined period of time. The scope of these incidents may include incidents affecting a third-party service or service provider on which the financial institution relies. Accurate and early assessments of incidents can be difficult if third-party service providers do not share relevant incident information with financial institutions in a timely manner, notwithstanding service providers' efforts to remediate the incident. The FSB's Recommendations to Achieve Greater Convergence in Cyber Incident Reporting (CIR Recommendations)[34] emphasise the need to balance timely reporting with remediating operational challenges that could detract from incident response.

Financial institutions may want to consider the overall quality of a third-party service provider's incident response programme in their due diligence and monitoring, consistent with the criticality of the services they provide. Financial institutions may also wish to engage with third-party service providers to raise awareness of the value and importance of incident reporting, better

---

33 The use of the term "incident" is intended to be inclusive of, and thematically consistent with, the FSB's definition of cyber incident: An [an observable occurrence] that adversely affects the [the preservation of the confidentiality, integrity and availability] of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not. The term "incident" in the document is not limited to cyber incident but captures a wider scope relevant to third-party risks.

34 At the request of the G20, the FSB has published in April 2023 Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, which sets out recommendations that aim to promote convergence among CIR frameworks for financial institutions, while recognising that a one-size-fits-all approach is not feasible or preferable. The CIR Recommendations include extensive discussions of cyber incidents impacting third-party service providers to regulated financial institutions.

understand possible challenges faced by third-party service providers and identify approaches to overcome them, ideally before an incident takes place.

Financial institutions may require third-party service providers to have clearly defined processes for identifying, investigating, remediating and notifying the financial institution in a timely manner of incidents that impact the third-party service provider's ability to deliver agreed-upon services or other obligations. The purpose of these requirements is to enable the financial institution to perform its own risk management, and where applicable, comply with any reporting obligations to authorities. The requirements imposed by financial institutions can be adjusted based on the criticality of the relevant service, and where appropriate, may also consider downstream impacts from an incident originating at a third-party service provider's wider supply chain.

Specifying incident reporting obligations in contracts can be an important tool for financial institutions.[35] Contracts may specify key criteria around the scope of reportable incidents, reporting timelines, and details to be reported. Financial institutions should consider applicable regulatory requirements when negotiating contractual provisions on incident reporting with third-party service providers. These obligations may, for instance, cover:

- The types of incidents requiring notification;
- The criteria to classify the severity of incidents, which may include but is not limited to their impact on:
  - Confidentiality, integrity, or availability of the financial institution's data (or that of its clients);
  - Continued delivery of a critical service according to agreed service levels and in line with the financial institution's tolerance for disruption of any critical operations that rely on that service; or
  - The financial institution's key legal or compliance obligations.
- The minimum information to be reported;
- The points of contact, channels, formats, and tools to be used for incident reporting;
- The timeframe for notifying the financial institution. This timeframe could vary based on a severity classification of incidents and/or the financial institution's applicable legal obligations to notify financial authorities of incidents within a certain timeframe; and
- Protocols for subsequent status updates.

CIR Recommendation 4 encourages financial authorities to implement phased reporting requirements for financial institutions, given that accurate and comprehensive information is difficult to produce early in a crisis scenario. Financial institutions may consider a similar phased

[35] In addition to specifying incident reporting obligations in contracts, financial institutions may also monitor the third-party's ongoing performance, in particular any failure by the third-party to meet contractual obligations to report incidents on a timely basis. Remedies for a failure to meet these requirements may include terminating the contract.

approach in their contractual requirements for third-party service providers, given that third-party service providers are likely to face the same operational challenges when reporting incidents.[36]

A financial institution may request that a third-party service provider supplies more frequent and detailed updates as an incident is being remediated. This could involve requirements to produce a final report identifying the cause(s) of the incident, commensurate with the severity classification and impact of the incident on the financial institution.

Financial institutions may consider developing a dedicated internal process for managing incidents originating at third-party service providers or integrate the identification, remediation, and reporting of a third-party incident into broader processes and reporting lines responsible for managing internal operational incidents within the financial institution.

3.4. Financial institutions' registers of third-party service relationships

Clear, consistent mapping of third-party service relationships can support financial institutions' effective monitoring and management of third-party risks. It can also provide useful data for financial authorities to identify systemic third-party dependencies and related potential systemic risks (see Chapter 4).

Financial institutions may:

- Keep a full, up-to-date, register of their third-party service relationships that identifies the criticality of different services;
- Make the register, or parts thereof, available to financial authorities periodically,[37] upon request or in specific circumstances, such as (i) a new or proposed arrangement or (ii) a significant change to an existing arrangement for the provision of critical services; and
- As part of their operational resilience framework, map the necessary dependencies and interconnections for the delivery of their operations supporting critical services, including those dependent on intra-group arrangements and service providers.

Financial authorities may have different current and evolving expectations as to what specific information financial institutions should set out in such registers. However, this information could include elements such as:

- A brief description of each third-party service relationship and (if available) a unique identifier for each service provider (e.g. legal entity identifier (LEI));[38]

---

36 The CIR Recommendations noted that global financial institutions are subject to a diverse and fragmented array of incident reporting obligations, which has the potential to detract from incident response. In one case, a global bank was applicable to dozens of different reporting obligations on short timeframes. Some third-party service providers, particularly those operating across economic sectors and jurisdictions, may be required to provide information to clients that are subject to an even more diverse array of requirements. See also FSB Chair's letter to G20 Finance Ministers and Central Bank Governors: April 2023.

37 This and other information could be provided to financial authorities confidentially, as appropriate, in order to avoid risks potentially arising from public disclosure.

38 See FSB (2019), *Thematic Review on Implementation of the Legal Entity Identifier: Peer Review Report*, May.

- A list of all third-party service relationships that the financial institution has identified as providing a critical service and a brief explanation of the financial institution's rationale for doing so;
- Listing of key nth-party service providers; and
- Whether the financial institution is sharing confidential, personal, regulatory or otherwise sensitive data with the service provider and, if so, who is processing that data, where and how.

3.5. Management of risks from service providers' supply chains

3.5.1. General expectations

Financial institutions may:

- Identify risks to critical services relating to third-party service providers' supply chain; and
- Implement appropriate and proportionate measures to monitor, manage and mitigate these risks that may affect the delivery of critical services.

Third-party service relationships often involve indirect reliance on other entities in the third-party service provider's supply chain (nth-party service providers) for the delivery of services to financial institutions. This indirect reliance should not lessen the regulatory responsibilities and accountability of financial institutions. Third-party service providers, through their own management of third- and nth- party risks, may have appropriate processes in place to address supply chain risks that may impact their ability to deliver services in line with contractually agreed service levels. As part of due diligence and ongoing monitoring, financial institutions may assess the effectiveness of these processes to determine if additional actions may be appropriate. For example, contracts between financial institutions and third-party service providers may cover whether the latter may sub-contract critical services (or parts thereof) and, if so, subject to which conditions.

Addressing risks associated with service providers' supply chain in a risk-based manner is one of the most significant ongoing practical challenges for both financial institutions and service providers. Given the growing complexity and length of service providers' supply chains, particularly in areas such as ICT, it can be impractical for each financial institution to directly assess and manage every unique risk across each element of their third-party service providers' supply chains. Consequently, this section of the toolkit recognises the need to apply the principle of proportionality in the management of risks from key nth-party service providers. In particular, the toolkit acknowledges that there are practical limitations to financial institutions' ability to directly monitor and manage these risks. For instance:

- Gaps in the information provided by third-party service providers;
- The cost, resourcing and time implications for financial institutions of identifying and monitoring third-party service providers' use of nth-party service providers; and

- Limited ability for financial institutions to influence third-party service providers' use of nth-party service providers and to access, audit and obtain information from these nth-party service providers.

- The inability of financial institutions to directly oversee their third-party service provider's nth party service providers, and the corresponding need for financial institutions to rely on their critical service providers to:

    - implement an appropriate supply chain risk management framework;

    - provide clear, complete and timely information to financial institutions about their key nth-party service providers, in particular, in cases of disruption.

For service providers, particularly those that provide services to many different entities, there are similar practical limitations, particularly around cost, resourcing and time. For instance, service providers have to balance potentially competing considerations, such as the concerns of their customers and the need to ensure the confidentiality of sensitive supply chain information. Small and medium-size service providers may face additional practical limitations, given limited influence over nth-party service providers, particularly when the nth-party service provider is further down in the supply chain. In light of these challenges and limitations as described below, the toolkit should be applied in a proportionate, and risk-based manner.

As noted above, the focus in this section is on key nth-party service providers that are critical to the delivery of a critical service by a third-party service provider to a financial institution or have the ability to access sensitive or confidential financial institution information (e.g. consumer data). Consequently, the failure or disruption of the services of an nth-party service provider could disrupt or otherwise create significant risks to the critical services consumed by a financial institution. Consistent with the principle of proportionality and a risk-based approach, financial institutions and third-party service providers alike should develop approaches to identify key nth-party service providers and develop appropriate risk management strategies to identify and address risks they may pose.

In many cases, key nth-party service providers might be direct sub-contractors of the third-party service provider (i.e. fourth-party service providers). However, key nth-party service providers might also be found further down the supply chain. Focusing on those nth-party service providers that are knowingly essential to the delivery of critical services to financial institutions or which have access to confidential or sensitive data belonging to the financial institution can be more consistent with a proportionate, risk-based approach. Financial institutions can assess how a critical service provider understands and assesses its supply chain to identify such key nth party service providers. Effective and proportionate risk management strategies for this area continue to evolve, given the inherent practical limitations described, and so financial institutions may also consider alternative risk-based tools other than those described below to mitigate the risks posed by key nth-party service providers, if these tools can achieve similar or better outcomes.

3.5.2. Information

Appropriate visibility of third-party service providers' key nth-party service providers is important for financial institutions' risk monitoring and management.

Financial institutions may, as part of their due diligence and subsequent ongoing monitoring, require that third-party service providers provide them with appropriate, up-to-date information about their key supply chain dependencies relevant to the delivery of critical services, or which may carry a higher level of risk as determined by the financial institution. An illustrative example of the information that service providers may provide is a software bill of materials from software suppliers, such as a list of software libraries that comprise the software and that are not strictly related to the relevant third-party service relationship (e.g. open source).[39] Additionally, financial institutions may wish to consider whether the length or complexity of a third-party service provider's supply chain may pose challenges to a financial institution's due diligence and ongoing monitoring.

Third-party service providers may update the information they provide to financial institutions about their dependencies on key nth-party service providers. For instance, a third-party service provider may inform a financial institution of plans to sub-contract a key part of a critical service to a new sub-contractor. These updates would give financial institutions enough time to assess new or increased risks and implement appropriate risk mitigation.

3.5.3. Contractual provisions

Financial institutions and third-party service providers may agree on certain provisions to monitor and manage supply chain risks in their contracts for critical services in a proportionate and risk-based manner, including but not limited to:

- A commitment by third-party service providers to ensure that nth-party service providers, in particular those that are key to the delivery of the critical service, meet appropriate resilience and service standards, including by implementing an appropriate supply chain risk management framework.
- To grant financial institutions the rights to:
    - Have access to, and as appropriate audit, information on third-party service providers' supply chain risk management. For instance, audit reports, certifications or the results of tests (e.g. scenario tests involving disruption at a key nth-party service provider);
    - Be notified promptly of supply chain disruption impacting critical services or posing significant risks to the confidentiality, integrity or availability of their data; and
    - Receive timely notification of planned changes to key nth-party service providers.

3.5.4. Other tools for mitigating supply chain risks

Financial institutions' registers of third-party service relationships may include:

[39] See G7 (2022), *G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*, October.

- A list of key nth-party service providers, such as those deemed critical to the continuity of the critical service(s) they receive, or to the viability of the third-party service provider; and

- If available, continuous monitoring of data facilitated by the third-party service provider as a potential tool to monitor and manage supply chain risk.

There may be instances where a financial institution has both a direct and indirect reliance on the same service provider, i.e., the service provider is both a third-party service provider and an nth-party service provider to other third-party providers that the financial institution relies on. Where this is the case, financial institutions may consider these overlapping dependency relationships in their risk management.

3.6. Business continuity

3.6.1. General expectations

Clear, up-to-date and appropriately tested business continuity planning to address the continuity of critical services is key to safeguarding the operational resilience of financial institutions. In particular, financial institutions may:

- Implement, maintain and regularly test business continuity plans to anticipate, withstand, respond to, and recover from the disruption or failure of critical services; and

- Seek to ensure that their relationships with third-party service providers commit them to:

    - Implement appropriate business continuity plans (and other relevant plans such as contingency plans, disaster recovery plans and incident response plans) covering critical services they provide to the financial institution;

    - Regularly test these plans and share the results, including lessons learnt, vulnerabilities and remediation actions; and

    - Support the testing of financial institutions' business continuity plans as appropriate.

Both financial institutions' and third-party service providers' business continuity plans may incorporate business impact analyses (BIA), recovery strategies, testing programmes, awareness and training programmes, and communication and crisis management programmes.

Business continuity plans should be distinguished from exit plans examined in the next section, which are a distinct process with different objective. However, some business continuity plans may include an exit from the third-party service relationship where feasible, practicable and usually as a measure of last resort.

3.6.2. *Financial institutions' business continuity plans*

Financial institutions' business continuity plans may focus on their ability to maintain operations following severe but plausible disruption to a critical service. Plans need to be forward-looking when assessing the impact of potential disruption.

Financial institutions may start developing their own business continuity plans for critical services (and assessing the business continuity plans of prospective service providers) at the onboarding stage using the tools in Section 3.2. Doing so can help inform financial institutions' choice of third-party service provider and (if relevant) how they configure and use critical services. For instance, in the case of data and infrastructure, financial institutions may have options including but not limited to:

- Using multiple data centres, whether from the same geographical region or spread across multiple regions;
- Combining on-premise and external (non-exclusive) data centres;
- Using multiple service providers, or a primary and back-up provider;
- Retaining the ability to bring data or applications back on-premises; or
- Any other viable options that can deliver a level of resilience consistent within the financial institution's risk appetite and tolerance for disruption.

All of the above measures have advantages and limitations, which financial institutions should assess on a case-by-case basis. Limitations may include but not be limited to costs, complexity, interoperability issues, legal and regulatory challenges.

Financial institutions may approach the development of their business continuity plans for critical services as a continuously evolving process rather than as a point-in-time exercise. Financial institutions may regularly test their business continuity plans against severe but plausible scenarios that incorporate disruptive events and incidents. They may also update their business continuity plans periodically to incorporate:

- Lessons learnt from incidents and testing;
- Feedback from advisers, industry groups, service providers, financial authorities etc.; and
- Changes in industry practice or technology that may impact available options for ensuring business continuity (e.g. by making services more substitutable).

3.6.3. *Third-party service providers' business continuity plans*

Financial institutions may ensure that third-party service providers:

- Develop and maintain business continuity plans informed by a comprehensive BIA, and set out clear, measurable indicators (e.g. RTOs, RPOs, maximum potential loss). Indicators used by third-party service providers could complement and support those

used by financial institutions in their business continuity plans, in particular where financial authorities require financial institutions to meet specific RTOs;

- Regularly test their business continuity plans and share relevant findings (including vulnerabilities), lessons learnt, and remediation actions planned or undertaken; and

- Conduct joint business continuity testing with financial institutions (individually or collectively), where appropriate and feasible.

Recognised certifications and standards can provide comparable, partial assurance. However, third-party service providers may need to be prepared to provide more detailed information where appropriate, including guidance to financial institutions on ways to optimise their business continuity plans. Any limitations on the provision of information to financial institutions may be confined to what is strictly necessary for the third-party service provider to preserve its intellectual property, security or confidentiality obligations to other clients.

3.7. Exit strategies

Financial institutions may consider identifying, documenting and, to the extent possible, testing exit strategies for their third-party service relationships involving critical services. Exit strategies can cover a range of scenarios, including normal and planned migrations of services and service providers but also adverse events, such as:

- A significant breach, or recurrent breaches, of applicable laws, regulations or contractual terms by a third-party service provider;

- A deterioration in the quality of the services provided by a third-party service provider;

- Weaknesses in the third-party service provider's governance, financial condition, resilience or risk management that have impacted or could reasonably impact the delivery of critical services; and

- Extended disruption to critical services that cannot be managed through other business continuity measures – though exit strategies are unlikely to be a feasible response to short-term severe disruption, which might be best managed through the business continuity tools in the previous section.

Financial institutions may appropriately plan, execute and oversee an exit from a critical service relationship by ensuring that there are appropriate:

- Contractually agreed transitional periods to minimise the risk of disruption;

- Processes to ensure that, where applicable, the financial institutions' logical assets (e.g. data and applications) and physical assets are returned in a cost-effective and timely manner, and in a format that allows them to continue their business operations; and

- Provisions relating to the ownership, maintenance, preservation, and long-term availability of records (including audit trails and other regulatory records).

In addition to fulfilling all their contractual obligations, third-party service providers may provide all reasonable assistance to financial institutions during the transition period following an exit.[40]

There is no one-size-fits-all approach to exit planning. Financial institutions' can enhance the effectiveness of their exit plans by bringing together decision-makers across the institution to collaboratively agree what measures to take. Financial institutions may prioritise the continued performance of critical operations and identify all viable forms of exiting critical third-party service relationships, which may include but not be limited to bringing the data, function and/or service back in-house/on-premises, or transferring them to an alternative or back-up service provider. The feasibility of an exit plan may depend on the circumstances of the financial institution, the relevant critical service and the service provider. Exit strategies that are designed to be implemented over longer time periods may not be as useful to address significant short-term disruption to critical services that cannot be remediated through other business continuity measures. These exit strategies may, however, facilitate a controlled, planned exit over a suitably long timeframe, which can help mitigate the risk of disruption that is often associated with change management initiatives. Conversely, developing capabilities to exit critical third-party service relationships in a short timeframe and without undue risks in unplanned, stressed circumstances, could increase the substitutability of that service and increase the resilience of the financial institution to certain events. On the other hand, some critical services are challenging to substitute and developing options to exit over a short-term may not always be feasible without undue costs or risk to the financial institutions.

3.8. Management of concentration-related risks by individual financial institutions

While the toolkit notes the relevance of concentration, it does not propose a singular and prescriptive manner for individual financial institutions to assess concentration or concentrated-related risks. Additionally, the criticality of different critical services is not binary or equal (e.g. one critical service from one service provider may be significantly more material to one institution than three critical services at another institution).

Financial institutions may choose to increase their use of a given service provider for various reasons, including internal expertise or synergies in deployment of a particular business model or for risk management efficiencies and effectiveness. These attributes can strengthen financial institutions' resilience and improve the efficiency and flexibility of their operations.

At the same time, critical services (or in some cases, a combination of critical and non-critical services) provided from the same service provider may be subject to the same set of risks, and may increase the overall impact of a disruption to any institution, creating concentration and concentration-related risks for individual financial institutions, examined in Section 3.8,[41] and systemic third-party dependencies and potential systemic risks (examined in Chapter 4).[42]

---

40 Data protection laws in certain jurisdictions may impose specific requirements regarding the handling of data following contractual termination, such as data retention requirements on the service provider.

41 It also considers certain forms of concentration and concentration-related risk for individual financial institutions that may not involve a specific service provider. For instance, a financial institution may be unduly reliant on a jurisdiction or region, such as an offshoring hub, for certain services, including critical services.

42 See Financial Stability Institute (2022), *Safeguarding operational resilience: the macroprudential perspective*, August.

Therefore, institutions may consider the overall concentration in services as a relevant factor in the risk management of critical services.

3.8.1. Identification of concentration-related risks within individual institutions

Concentration and related risks at a financial institution may arise from a combination of factors, including through:

- The overall number of services supported by a single or closely connected service providers;
- The number of critical services supported by a single or closely connected service providers (sometimes referred to as “aggregation”); and/or
- Exposure to certain jurisdictions or regions.

3.8.2. Mitigation of potential concentration-related risks

Financial institutions may consider identifying and assessing concentration (including, where relevant, on a group basis) in the services they receive from both third-party service providers and their key nth-party service providers; and establishing adequate measures to mitigate these risks. In some scenarios, financial institutions may judge that the risks of relying on a market-leading service provider for a critical service are lower than the risks of delivering the critical service in-house or relying on a different or multiple service providers for it.

Financial institutions can manage concentration and concentration-related risks by deploying the potential tools in the toolkit in a manner commensurate with the overall level of criticality of a concentration, including:

- Enhanced due diligence and oversight of service providers deemed to pose such a risk during onboarding and ongoing monitoring (see Section 3.2);
- Mapping of concentration risks, including those arising from service providers’ supply chains (see Sections 3.1 and 3.4);
- Inclusion of information on the concentration and substitutability of services in their registers of third-party service relationships (see Section 3.4);
- Steps to ensure that service providers can meet their needs both during business-as-usual and in stressed circumstances (e.g. disruption, unusual market activity), for instance, by including service providers in the testing of their business continuity plans (see Section 3.7);
- Contractual rights, where appropriate and feasible, regarding the sub-contracting of parts of a critical service that may increase risk (see Section 3.5);
- Requesting critical services which are provided by a single service provider, to be provisioned from multiple availability zones or multiple regions whenever possible, to avoid operational or geographical concentration risks; and

- Where appropriate and feasible: retaining the ability to bring the critical service back in-house; choosing different service providers for different critical services; designating a primary and backup service provider for a critical service; and maintaining a list of viable potential alternative service providers. However, financial institutions may weigh the potential benefits of multi-vendor approaches against potential drawbacks, unintended consequences and risks.

4. Financial authorities' oversight of third-party risks

This chapter sets out financial authorities' current and developing approaches and tools for:

- Supervising how financial institutions manage third-party risks; and
- Identifying and monitoring systemic third-party dependencies, and potential systemic risks and managing those risks, which could arise, for instance, due to disruption to certain services or the financial or operational failure of service providers. In some jurisdictions this may involve authorities designating certain third-party service providers as critical to the financial sector from a financial stability perspective (hereafter "financial sector critical service provider") and directly overseeing the resilience of their services to financial institutions.[43]

For ease of reading, the term "systemic third-party dependencies" is mainly used in the document. However, taking into account the abovementioned approaches in some jurisdictions, the toolkit is applicable to third-party service providers designated as "financial sector critical service providers" in some jurisdictions.

4.1. Financial authorities' supervision of financial institutions' third-party risk management

Most jurisdictions already cover outsourcing in their regulations and supervision. In addition, several financial authorities have recently modernised their frameworks to encompass third-party service relationships more holistically in line with the approach in this toolkit.

Financial institutions must ensure, usually through contractual means, that their third-party service relationships allow them to meet their regulatory responsibilities. This includes financial institutions (including their designated agents) having appropriate access, audit, and information rights relating to the relevant service(s). To the extent required in the regulatory framework, such rights are provided for financial authorities (including their designated agents). This may be ensured in contracts between financial institutions and their service providers or, in certain jurisdictions, through direct requirements or expectations on financial sector critical service providers. Financial institutions may occasionally find themselves in a weaker negotiation position relative to certain third-party service providers. Where this is the case, clear regulatory

[43] In these jurisdictions, a "financial sector critical service provider" is defined as a service provider to financial institutions whose services have been deemed by financial authorities to give rise to a systemic third-party dependency with potential implications on financial stability, including potential systemic risk case of disruption or failure. This is a general concept, and the specific term and definition may differ depending on jurisdictions.

and supervisory expectations by authorities about what contracts for critical services should include, where appropriate, can help partially level the playing field.

Financial authorities may also obtain assurance about the resilience of service providers and the services they provide to financial institutions through:

- Regular supervisory engagement with financial institutions, including ad-hoc information requests, individual and horizontal reviews of financial institutions, and reviews of the assurance and information that financial institutions receive from service providers, including (if appropriate) the results of independent audits or collaborative assurance exercises, such as pooled audits.
- Informal (often voluntary) dialogue with service providers.

In a small, but growing, number of jurisdictions, financial authorities have gained (or are in the process of gaining) powers to directly oversee the provision of services to financial institutions, by financial sector critical service providers. These powers do not replace the regulatory obligations of financial institutions or financial authorities' supervision of financial institutions' third-party risk management. They do, however, complement these tools with the aim of monitoring and managing systemic third-party dependencies and potential systemic risks (see Annex 2).

4.2. Incident reporting to financial authorities

Incident reporting by financial institutions is an important tool for financial authorities as it can provide them with important data and actionable insights to fulfil their objectives, including effectively supervising financial institutions, and monitoring and managing potential financial stability risks.

As discussed in Section 3.3, the CIR Recommendations examine the need for, and usefulness of, cyber-incident reporting for financial institutions. The toolkit in this document is consistent with these recommendations and builds upon them with respect to incidents (including but not limited to cyber-incidents) at third-party service providers that impact their client financial institutions. Like the CIR Recommendations, the toolkit seeks to avoid unnecessary fragmentation in reporting requirements. Financial authorities should refer to the CIR Recommendations for specific recommendations and tools on the reporting of cyber incidents more broadly.

4.2.1. Current practices

In recent years, different regulatory and supervisory practices have emerged, and continue to evolve, in relation to incident reporting to financial and cross-sectoral authorities. As discussed in Section 3.3, in many jurisdictions financial institutions are required to report incidents meeting pre-determined criteria or thresholds, including cyber incidents, to one or more authorities.[44]

[44] The CIR recommendations include a description of different types of triggers that FSB members were using in 2022, though incident reporting requirements are being updated in a number of jurisdictions.

These requirements include incidents linked to a financial institution's third-party service relationships. The CIR Recommendations encourage financial authorities to:

- Provide sufficient detail to financial institutions (Recommendation 7);
- Promote timely reporting under relevant materiality reporting thresholds and triggers (Recommendation 8);
- Review the sufficiency of cyber incident reporting and cyber incident response and recovery procedures at financial institutions, where appropriate (Recommendation 9); and
- Protect sensitive information, given the potentially heightened risks of disclosure of this type of information (Recommendation 16).

In some jurisdictions, there are dedicated reporting frameworks whereby financial institutions can notify financial authorities of significant incidents, including those involving their third-party service providers. Financial authorities can then share this information with other regulatory bodies. In other jurisdictions, there are cross-sectoral reporting mechanisms as part of critical infrastructure legislation that include but are not limited to the financial services sector. Under these mechanisms, both financial institutions and service providers report relevant incidents through a cross-sectoral mechanism. These reporting mechanisms may operate in addition or as an alternative to frameworks for financial institutions to report incidents to financial authorities. As discussed in Section 4.3, in some jurisdictions, service providers could be asked to provide information directly to financial authorities, which may include information regarding incidents impacting their financial institution clients.

4.2.2. Enhancing financial authorities' understanding of incidents involving systemic third-party dependencies

An incident affecting critical services at multiple financial institutions could quickly give rise to potential financial stability risks warranting:

- Intervention by the financial authorities;
- Crisis communications by service providers, financial institutions affected by the incident and the financial authorities; and
- Communication and coordination between the financial authorities and relevant government or international stakeholders.

It is therefore critical that financial authorities receive accurate, actionable and timely information about an incident to enable them to implement appropriate tools and mitigating measures, while minimising obligations that could detract from the incident response of financial institutions and/or third-party service providers. Promoting the timely and effective use of available incident reporting tools is in the interest of both financial institutions and third-party service providers. While financial institutions will likely report these incidents to financial authorities in due course through the reporting channels discussed in Section 3.3 and the CIR Recommendations, financial authorities may want to consider how this reporting can be enhanced as needed, or

building channels to include relevant third-party service providers if the incident could potentially give rise to financial stability risks.

There are a number of means by which financial authorities can strengthen the quality of existing incident reporting requirements or consider enhanced approaches involving systemic third-party dependencies. However, it is important to note that a one-size-fits-all approach is not feasible given the different roles and legal authorities in various jurisdictions.[45]

Possible tools for authorities to consider include:

- Communicating with financial institutions to clarify the scope of reporting involving third-party services (CIR Recommendation 8) and to foster mutual benefits of reporting (CIR Recommendation 12);
- Carrying out ad-hoc information requests to financial institutions as appropriate, to complement the CIR reporting requirements (CIR Recommendation 10);
- Encouraging financial institutions to coordinate on a sector-wide basis to produce a common picture for financial authorities on incidents at third-party service providers affecting multiple financial institutions via engagement with sector response frameworks (if applicable – see Section 4.4.2);
- Encouraging service providers to give financial authorities access to the same or similar dashboards, portals etc. that their financial institution clients have access to so they can have real-time updates on incidents that may disrupt the provision of critical services to multiple financial institutions;
- If the service provider has a pre-existing legal obligation to notify another authority outside the financial sector in the jurisdiction(s) where the incident occurs (e.g. a cybersecurity or data protection agency), or in other jurisdictions, the service provider could consent to or request that authority to share the notification with the financial authorities, or do so directly (if legally permissible); and
- Third-party service providers could also be encouraged to share information with their contacts at the financial authorities through any form of communication (formal or informal) that is effective, secure, and ensures confidentiality, in order to help financial authorities assess whether direct action by authorities is necessary (such as coordinated use of tools like liquidity assistance or market calming measures etc.) and to forestall actions that may impact financial instability. To ensure a resource-efficient risk-based approach, this direct sharing of information to authorities could be limited to financial sector critical service providers and systemic third-party dependencies; and incidents that could impact financial stability. Service providers may not be able to fully assess the financial sector-specific impact of a given incident affecting their services, but may be able to estimate it using proxy measures such as

[45] Additionally, some third-party service providers already may have incident reporting requirements to other government entities, which financial authorities can consider in terms of the need for their direct engagement with third-party service providers.

- the number of their financial institution customers impacted, and the potential nature of the impact on customers, if known;
- the expected recovery time; and/or
- the nature of the incident.

There are also emerging frameworks (see Section 4.3) where financial authorities may have direct oversight of financial sector critical service providers and/or the services they provide to financial institutions. Financial authorities considering such an approach could consider how to adapt the CIR Recommendations for financial institutions, as appropriate, to promote effective practices for incident response without unduly preventing third-party service providers from focusing on remediation.

4.3. Financial authorities' identification, monitoring and management of systemic third-party dependencies and potential systemic risks

4.3.1. Overview

This part of the toolkit focuses on cases where financial authorities identify systemic third-party dependencies and, in some jurisdictions, financial sector critical service providers.

Not all critical services and service providers identified by individual financial institutions will be deemed by financial authorities to give rise to systemic third-party dependencies. However, individual financial institutions' assessment of critical services can provide a useful starting point for financial authorities. In principle, what renders a third-party dependency systemic is a financial authority's assessment of the potential impact on financial stability from disruption to the relevant service(s) or service provider.

In some jurisdictions or regions, financial authorities have or are in the process of acquiring regulatory powers to (i) formally designate certain service providers as financial sector critical service providers if they identify that their services to financial institutions give rise to systemic third-party dependencies; and/or (ii) oversee risks associated with these service providers and/or their services to financial institutions (see Annex 2).[46, 47] A number of jurisdictions do not currently have legal powers over either services or service providers and rely solely on the tools in Chapter 3. Irrespective of their approaches, financial authorities can leverage the tools in Section 4.3 as well as continuing to rely on those in Chapter 3. There is no preference in the toolkit for any particular approach, mindful that in all cases tools should be applied consistent with the principle of proportionality.

Where financial authorities identify systemic third-party dependencies, they may also assess whether they give rise to systemic risks. These risks could crystalise, for instance, if a systemic

---

46 Comparable terms include "critical ICT third-party service provider" in the EU and "critical third-party (CTP)" in the UK.

47 Even if the financial authority focuses on the services being provided, naturally any assessment of a service must involve certain elements of assessments of the service provider, or core infrastructure that contributes to the specific service(s) being provided in the financial sector.

third-party dependency experienced disruption or failure that affected multiple financial institutions simultaneously or one or more SIFIs. Individual financial institutions may be unable to adequately manage these systemic risks using just the tools in Chapter 3. Therefore, the use of additional tools by financial authorities, including but not limited to those examined in Section 4.3, might be warranted in these cases. In assessing potential systemic risks, financial authorities may consider:

- The impact on financial stability of the failure or severe disruption of a systemic third-party dependency, which may in turn be influenced by the:
  - Criticality of the relevant service provider and its services to financial institutions; and
  - The systemic significance of the financial institutions that rely on the relevant service provider and its services.
- Factors that could increase the likelihood or severity of such failure or disruption, including but not limited to weaknesses in the service providers' financial and operational resilience, and the criticality, recoverability or substitutability of its services to financial institutions; and
- Steps that could mitigate the likelihood or severity of such failure or disruption, including but not limited to risk management, response and recovery and business continuity measures taken by financial institutions, service providers and/or financial authorities either individually or collectively. For instance, through frameworks set up to promote a coordinated response to incidents impacting the financial sector (see Section 4.4).

4.3.2. Criteria for identifying systemic third-party dependencies and potential systemic risks

Financial authorities are primarily responsible for identifying potential risks to financial stability in their jurisdictions. Moreover, they are best positioned to identify and assess systemic third-party dependencies and potential systemic risks arising from such dependencies to different types of financial institutions (e.g. banks, insurers, pension funds).

The level of market concentration in a single or small number of service providers is relevant when identifying systemic third-party dependencies and potential systemic risks but is not the only consideration. Other relevant considerations include the criticality of service(s) provided by a service provider, the degree of substitutability of these services, and the systemic significance of the financial institutions that depend on these services.

Critical services are likelier to cause greater and more measurable impacts to financial institutions and, by extension, financial stability if disrupted. However, when assessing systemic third-party dependencies and (if relevant) identifying financial sector critical service providers, financial authorities may also consider relevant, non-critical services. For instance, this may be relevant when assessing the potential impact of the failure of a service provider that provides a mix of critical and non-critical services to financial institutions, or the simultaneous disruption of many or all of its services.

The criteria below can help financial authorities identify systemic third-party dependencies and assess and manage potential systemic risks. The criteria are non-exhaustive but could promote comparable approaches across jurisdictions, which may in turn facilitate cross-border cooperation (see Section 4.4). The criteria should be applied dynamically, as the criticality of a service or the level of market concentration on a service provider can vary over time.

Identification of systemic third-party dependencies

As an initial step to identify systemic third-party dependencies, financial authorities can produce a list of critical service providers and the critical services they provide based on data and information collected and pooled from the financial institutions they supervise. The registers referred to in Sections 3.4 and 4.3.3 of the toolkit can inform financial authorities' analysis. In the absence of these registers, or to complement or validate them, financial authorities can leverage other available relevant sources of information, for instance:

- Financial authorities that have implemented the Basel Committee Principles for Operational Resilience[48] in their jurisdiction may review banks' maps of "the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations", which should include "those dependent upon, but not limited to, third parties";

- Where applicable, financial institutions' recovery and resolution plans (in particular, the sections relating to operational continuity in resolution), which tend to list critical services and service providers, albeit often only those that may need to continue operating in the event of the financial institution's resolution; and

- Financial authorities may also consider other criteria and data sources.

Assessment of market concentration

Market concentration[49] in the provision of services to financial institutions is not a new phenomenon nor does it automatically pose systemic risks by itself. In some instances, it can strengthen the operational resilience (including cyber-resilience) of financial institutions and, by extension, financial stability.

However, relying on a single or small number of service providers will likely increase the impact to the financial sector if these service providers or their services to financial institutions (in particular, critical services) are disrupted or fail. Concentration combined with other criteria, such as the financial and operational resilience of the service provider, and the substitutability of its services, can be relevant considerations when identifying systemic third-party dependencies and potential systemic risks.

---

48 See BCBS (2021), *Principles for Operational Resilience*, March.

49 The "market" may not necessarily be limited to the financial sector.

Although financial authorities' assessment of concentration for the purpose of identifying systemic third-party dependencies will vary based on the characteristics of the financial sector in their jurisdictions, the following factors can be considered:

- Number and composition of services: The number, composition and characteristics of critical and, if feasible, non-critical services that financial institutions obtain from a single or interrelated group of service providers.
- Number of financial institutions clients served and systemic significance thereof: The overall number of financial institutions served, and the extent to which they include globally or domestically SIFIs.
- Interdependencies and indirect dependencies: When identifying systemic third-party dependencies, financial authorities may consider the service provider's supply chain used for the delivery of services to financial institutions. However, not all parts of a service provider's supply chain will be critical or even relevant to their provision of critical services to financial institutions (see Section 3.5). Financial authorities may also examine potential interdependencies between critical services. For instance, whether a single service provider supplies a range of critical services to financial institutions or if multiple critical services depend on a common infrastructure that is not easily severable or substitutable.

Characteristics that may increase the impact of disruption to critical services

When identifying systemic third-party dependencies, financial authorities can consider how severe disruption to the relevant services and service providers could impact the:

- Stability of, and confidence in the financial system;
- Continuity, quality, or stability of the provision of financial services by financial institutions, including impact on consumers;
- Safety and soundness of multiple financial institutions; and
- Stability and integrity of financial markets.

The extent to which disruption may impact one or more financial institutions may partly depend on their configuration of the relevant critical services and their individual and collective risk mitigation, response, recovery and business continuity capabilities.

The recoverability or substitutability (or lack thereof) of critical services and/or service providers may also impact positively or negatively on the potential systemic impact of their failure or disruption. In this context, substitutability refers to the ability of financial institutions to replace critical services in a cost-efficient, timely manner and without undue risks. Recoverability or substitutability may also change over time due to developments in risk management, the operations of financial institutions and markets, and technology changes among others. If a service or service provider becomes more easily substitutable over time, financial authorities may reassess whether the relevant third-party dependency can still be considered systemic. Based on this reassessment, financial authorities may reprioritise their focus. In jurisdictions

where authorities designate financial sector critical service providers, these changes could also lead to a review of the continued appropriateness of this designation.

The identification of systemic third-party dependencies, financial sector critical service providers and potential systemic risks can be more effective if it includes consideration of an appropriate range of relevant sources of disruption or failure, such as:

- Operational disruption or failure: Financial authorities should assume that operational disruption will occur. However, the degree and severity of this disruption may depend on the characteristics and resilience of the critical services and service providers affected and on mitigating actions by financial institutions and service providers; and

- Deterioration to the service provider's financial position: As might be the case with financial institutions, such a deterioration could pose challenges to the continued delivery of critical services to financial institutions but can be mitigated with appropriate planning and safeguards similar to those covered in the FSB Guidance on Arrangements to Support Operational Continuity in Resolution.[50]

Interaction with existing cross-sectoral frameworks

When identifying systemic third-party dependencies, financial authorities may consider the extent to which certain critical services or service providers may already be subject to a level of regulation or supervision that addresses their concerns.

For instance, although energy and telecommunications providers may create systemic third-party dependencies for the financial sector (based on an objective assessment of relevant criteria), financial authorities may be able to rely on existing regulatory frameworks for these providers rather than deploying additional financial sector-specific tools.

Financial authorities may also coordinate with relevant, non-financial public authorities in their jurisdictions (e.g. those responsible for cybersecurity or data protection) to minimise regulatory fragmentation and promote resilience across sectors. This can be particularly important when responding to incidents affecting multiple critical infrastructure sectors in a jurisdiction including but not limited to financial services.

4.3.3. Tools for identifying systemic third-party dependencies

Comprehensive and reliable data are vital for financial authorities' identification of systemic third-party dependencies. Financial authorities can obtain such data through various tools, including but not limited to:

- Notification of third-party service relationships: Financial authorities may receive and review event-driven notifications from financial institutions in relation to inception, material change or termination of third-party service relationships involving the provision of critical services (including the use of sub-contracting for critical parts of the services):

[50] See FSB (2016), *Guidance on Arrangements to Support Operational Continuity in Resolution*, August.

- Review of financial institutions' registers: Financial authorities may periodically receive up-to-date registers of financial institutions' third-party service relationships, or parts thereof, (see Section 3.4) and review data on financial institutions' critical and/or non-critical services.

- Incident notification: Financial authorities may receive and review certain incident notifications affecting critical services or service providers (e.g. cybersecurity incidents) (see Section 4.2.2).

Greater consistency in the data that financial authorities collect on financial institutions' third-party service relationships (from registers and other sources mentioned in Section 3.5 and 4.3.2) can help financial authorities build a clearer, more consistent view of systemic third-party dependencies and systemic risks within and across jurisdictions (as well as facilitating the identification of financial sector critical service providers where appropriate). Greater consistency could also mitigate compliance costs for internationally active financial institutions, some of which must maintain multiple registers, or different versions of a single register, containing substantively identical data. However, full global alignment of the data that financial institutions' keep about their third-party service relationships and how they report it to financial authorities, including the frequency of reporting, may not be possible to achieve in practice.

4.3.4. Tools for financial authorities to identify and manage potential systemic risks

The tools below are designed to help financial authorities identify and manage systemic risks which may potentially arise from systemic third-party dependencies. Given the different legal and regulatory regimes across jurisdictions, these tools are versatile and can in principle be adopted through:

- Voluntary collaboration between financial authorities, financial institutions, and relevant service providers;

- Requirements or expectations on financial institutions, which they could reflect in their arrangements with relevant third-party service providers; or

- Direct requirements or expectations on financial sector critical service providers.

Financial authorities may also choose to set and calibrate tools differently to different types of service providers in line with the principle of proportionality.

Dialogue between authorities, financial institutions, and service providers

Financial authorities may initiate or increase their dialogue with financial institutions and financial sector critical service providers (within individual jurisdictions and on a cross-border basis) to identify sector-wide trends, best practices, challenges to financial authorities' ability to manage potential systemic risks and actionable ways to address these challenges.

Sector-wide exercises and incident response coordination frameworks

Participating in financial sector-wide and multi-sectoral exercises can be a valuable way to explore and improve the financial services ecosystem's collective ability to respond and recover

from disruption. Financial sector critical service providers are critical nodes in the financial system and can therefore substantially enrich the value and lessons learnt from these exercises through their direct participation.

Financial sector critical service providers may participate in initiatives aimed at strengthening the collective ability of the financial sector to respond to and recover from disruption. For instance, they may consider actively engaging in:

- Sector-wide exercises;
- Joint assurance activities (e.g. tabletop exercises), and
- Incident response coordination frameworks focused on the financial sector or on critical infrastructure sectors (including but not limited to financial services).

Sector-wide exercises can be led by financial institutions (often working collectively through trade associations), authorities (both financial and non-financial e.g. national cyber incident security response teams (CSIRTs)) or a combination thereof. They can involve participants from multiple jurisdictions using tools to facilitate cross-border exercises, such as the G-7 Fundamental Elements for Cyber Exercise Programmes[51].

A number of jurisdictions also have frameworks to promote a coordinated, financial sector-wide response to operational disruption. These frameworks can likewise be led by financial authorities, the private sector or a combination of the two. They often connect to cross-sectoral incident response frameworks and (if applicable) counterparts in other jurisdictions. Some examples include:

- Cross Market Operational Resilience Group (CMORG) and Financial Services Cyber Collaboration Centre (FSCCC) in the UK;
- Financial and Banking Information Infrastructure Committee (FBIIC) and Financial Services Information Sharing and Analysis Center (FS-ISAC) in the US; and
- The Unit for business continuity (Codise) and the Financial Sector Computer Emergency Response Team (CERTFin) in Italy.

Financial sector critical service providers may engage with these frameworks by:

- Nominating entities or individuals to coordinate with these frameworks in case of relevant disruption; and
- Developing and testing crisis coordination and communication plans for the financial sector, which can be integrated into their wider crisis coordination and communication plans.

---

51 See G7 (2020), *G7 Fundamental Elements for Cyber Exercise Programmes*, October.

4.3.5. Review by financial authorities

Financial authorities may consider reviewing information financial institutions maintain regarding their monitoring of critical services and service providers. Financial authorities may also consider conducting such an analysis on a horizontal, comparative basis across all, or a sample, of financial institutions that rely on critical services from the same service provider. When undertaking horizontal reviews, financial authorities should not necessarily view differences in financial institutions' approaches as a negative factor, as these differences may be inconsequential or justified.

Third-party service providers can also make available to financial authorities, if possible, the information that financial institutions leverage during their onboarding and ongoing monitoring, considering the legal requirements in the jurisdiction (see Section 3.2). Information such as independent reports can provide partial assurance to financial authorities about service providers' controls. Financial authorities can then judge whether this information provides sufficient assurance or whether additional information is needed to monitor and manage potential systemic risks. Where this is the case, financial authorities may identify and highlight to service providers key assurance and information gaps and potential ways to address them. For instance, in relation to service providers' assessments of the business continuity and reliability of their critical services to financial institutions.

Financial authorities could assess the resilience of financial sector critical service providers and their services against international, jurisdiction-specific or bespoke principles. For instance:

- Annex F of the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) outlines five oversight expectations for critical service providers[52] in order to support an FMI's overall safety and efficiency.
- The BCBS Principles for Operational Resilience, and BCBS Principles for the Sound Management of Operational Risk contain several principles directly and indirectly relevant to banks' use of critical services provided by service providers. It can be good practice, in particular for service providers whose services are deemed by financial authorities to give rise to systemic third-party dependencies, to consider whether the way they provide services to banks facilitates their compliance with these principles.
- The IOSCO Principles on Outsourcing (2021) comprise a set of fundamental precepts and seven principles for securities markets participants. The fundamental precepts cover overarching issues, in particular proportionality and the assessment of materiality and criticality. The seven principles set out expectations for financial institutions and include guidance for implementation, depending on the criticality and materiality of the third-party services. These principles are addressed to the wide range of participants in securities markets, including many small and medium size financial institutions, and therefore provide a proportionate set of expectations for both critical and non-critical third-party services.

---

[52] Annex F uses the term critical service provider exclusively for critical service providers to FMIs, which generally have a prominent role in the financial sector. For the purpose of the toolkit, the term has been broadened for application to a broader range of financial institutions.

4.4. Cross-border supervisory cooperation and information sharing

Cross-border supervisory cooperation and information sharing is valuable to support:

- Effective regulation and supervision of internationally active financial institutions' third-party arrangements; and
- The identification, monitoring and management of systemic third-party dependencies, and potential systemic risks, some of which may have a cross-border and even global component.

The value of cross-border supervisory cooperation and information sharing stems from several factors. For instance, as noted in Chapter 2, internationally active financial groups often centralise their use of critical services via an intra-group service provider, such as a service company, which enters into contractual arrangements with third-party service providers on the group's behalf and then cascades the relevant services to group entities. This approach can bring benefits to financial institutions, for instance, in a resolution scenario.[53] However, it also means that financial authorities responsible for supervising the financial group's entities around the world may have less visibility of the critical services that those entities receive, the third-party service providers they receive them from, or the group's business continuity plans should these third-party service providers experience disruption or failure.

Likewise, some third-party service providers supply services from different jurisdictions to those where their financial institution's customers operate, or from multiple jurisdictions. Divergences in legal and regulatory requirements and expectations, although inevitable in some cases, can increase compliance costs for service providers and even impact negatively on the resilience of their services. Moreover, where services are provided in a standardised way across jurisdictions, there can be efficiencies in financial authorities exchanging information about assurance and monitoring activities that they, or the financial institutions they supervise, undertake on service providers.

Finally, cross-border supervisory cooperation and information sharing can help financial authorities respond more effectively to incidents at a service provider that disrupt financial institutions in multiple jurisdictions. In particular, this is the case where the incident involves systemic third-party dependencies or poses potential systemic risks in multiple jurisdictions. For instance, there can be benefits if financial authorities exchange information about the disruption in real time or discuss remediation or risk mitigation carried out by them and/or financial institutions in their jurisdictions. Still, the potential benefits of real-time information exchange must be balanced against any downside resource impact this may have on financial institutions who may still be in the midst of incident response.

---

[53] As noted in the FSB's 2016 Guidance on Arrangements to Support Operational Continuity in Resolution, "to the extent that service provision under such arrangements is clearly documented, this is likely to facilitate mapping of services to recipient entities and provide greater clarity about which shared services need to continue in resolution. Such arrangements may also facilitate the restructuring of business lines or legal entities within the group as part of resolution". Further, supervisory colleges play an important role in enhancing coordination, information-sharing and in addressing risks and vulnerabilities of international banking groups (see BCBS Principles for effective supervisory colleges).

4.4.1. Challenges

Management of systemic third-party dependencies and potential systemic risks to the global financial system can be more effective with improved coordination, collaboration and information sharing among supervisors in multiple jurisdictions. As mentioned in Section 4.3, financial authorities in any given jurisdiction are limited in their ability to identify, monitor, and mitigate both systemic third-party dependencies and potential systemic risks posed by service providers operating internationally. However, there can be challenges to enhancing cooperation on third-party service relationships, such as:

- Differences in financial authorities' mandates, legislation, organisational structure and frameworks. Financial authorities in different jurisdictions typically have different regulatory frameworks, legal requirements, supervisory practices, and resourcing models. Their powers over third-party service providers (or a subset thereof such as financial sector critical service providers) can be significantly different;

- Practical challenges in coordinating supervisory activities across different jurisdictions to ensure greater consistency and effectiveness of oversight. In particular, where multiple regulators with a limited prior working relationship are involved; and

- Challenges in sharing sensitive information. Some information related to third-party providers might be highly sensitive and obtaining consent for certain access or information may be required depending on existing contractual clauses or other legal obligations. Sharing of confidential information without consent may expose financial authorities, financial institutions or the service providers to legal and reputation risks and inappropriate treatment of such sensitive information could lead to increased cyber security and other business risks.

4.4.2. Possible tools for improving cross-border supervisory cooperation and information sharing

Explore greater convergence of regulatory and supervisory frameworks around systemic third-party dependencies

To minimise fragmentation, improve interoperability, and promote financial stability, financial authorities can continue to explore ways to improve alignment of their regulatory and supervisory frameworks on third-party risk management on a cross-border and cross-sectoral basis. For instance, establishing more consistent criteria and methodologies for the assessment, classification and identification of systemic third-party dependencies and potential systemic risks could facilitate the exchange of information across authorities and promote more efficient oversight.

However, such alignment needs to accommodate specific authorities' cross-border (and cross-sectoral) information sharing constraints. Financial authorities may also explore mechanisms, subject to applicable legal frameworks governing the confidentiality of supervisory information, for securely exchanging and comparing data and information about critical services offered by service providers to financial institutions, and the identification of systemic third-party dependencies and potential systemic risks in their respective jurisdictions.

Effective cross-border cooperation could help inform individual authorities through risk-based exercises using the tools described in Section 4.3. For example, a tabletop exercise conducted by one authority could yield insights for other authorities.

Financial authorities may also take into account more elaborate assurance activities (such as inspections, sector-wide exercises and tests) and other relevant engagement carried out by or on behalf of financial authorities in other jurisdictions. Doing so could make more efficient use of financial authorities' resources, and from the perspective of the financial sector critical provider, minimise possibility of duplicate requests and avoid overlapping assurance activities where possible. This can be particularly efficient where:

- The critical services provided by the service provider to financial institutions in both jurisdictions are identical or sufficiently similar;
- The financial authority that undertook or arranged the assurance activity or engagement, shares relevant information; and
- The relevant assurance activity or engagement is deemed suitable for the objectives and needs of the financial authority or authorities receiving the information.

Explore options for greater cross-border information sharing

Financial authorities can consider exploring methods for collaboratively overcoming legal or confidentiality challenges relating to the cross-border exchange of relevant information on financial institutions' third-party risk management practices and, if applicable, assurance activities involving service providers. For example, financial authorities may be able to use Memoranda of Understanding (MoUs), or equivalent arrangements to set out the basis for the information exchange, which may include commitments to maintain the confidentiality of information.

While there are already MoUs and other cooperation arrangements among several financial authorities currently in force, in some cases they do not cover the exchange of information on unregulated service providers. Where this is the case, financial authorities can consider whether the collaborative development of additional clauses can enhance such MoUs and information exchanges.

Financial authorities could also explore additional models for international cooperation and information sharing (e.g. supervisory colleges, fora, networks).[54] Financial authorities could use similar cooperative oversight arrangements to share information on third-party service providers deemed financial sector critical service providers by authorities in multiple jurisdictions. If appropriate, these cooperation fora could include relevant non-financial authorities, such as those responsible for cyber-security and data protection. Discussions at these fora could include information on vulnerabilities and incidents subject to appropriate confidentiality and sensitivity safeguards. To further improve cross-border cooperation, financial authorities may explore the

[54] Such cooperative oversight arrangements already exist in the case of Society for Worldwide Interbank Financial Telecommunications (SWIFT) and, more recently, the Oversight Forum in the EU's DORA (expected to go live in January 2025).

benefits and applicability of regional or global structures to share information or promote regulatory cooperation regarding third-party services.

Explore cross-border resilience testing and exercises

There are several precedents for cross-border collaboration among financial authorities involving cross-border testing and sector-wide exercises of financial institutions. Bringing internationally active service providers into future cross-border and sector-wide exercises and, if appropriate, cyber resilience tests could help strengthen the resilience of the global financial system. To supplement them, financial authorities could see value in the external assurance/certification of service providers or the standardisation of contract terms, while due care should be taken for the level of assurance.

Table-top sector-wide exercises and/or global risk assessments could be considered as means for assessing the potential impact of the failure or disruption of critical services or systemic service providers and improving the coordinated response and recovery capabilities of financial authorities, financial institutions and critical third-party service providers.

On a longer timeframe, and subject to new or updated bilateral and multilateral cooperation arrangements, authorities, or groups thereof, could conduct joint examinations and other oversight activities, which could be particularly beneficial and resource-efficient in the case of common financial sector critical service providers.

Annex 1: Relevant Developments at the Standard Setting Bodies

BCBS

In March 2021, the Basel Committee on Banking Supervision (BCBS) issued Revisions to the Principles for the Sound Management of Operational Risk (PSMOR) and Principles for Operational Resilience (POR). [55] The PSMOR establish principles for operational risk management and the POR seek to promote a principles-based approach to strengthen banks' ability to withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets, such as pandemics, cyber incidents, technology failures or natural disasters.

The PSMOR recognise third-party arrangements (including outsourcing) as an important component of a bank's operational risk management framework and overall risk management programme. This is best illustrated by Principle 9 ("Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies"). Paragraph 54 outlines the responsibilities of the board of directors and the senior management in understanding and managing operational risk associated with outsourcing arrangements and provides a list of the key components of a robust outsourcing management framework.

In the POR, the reference to third-party arrangements is even more prominent. Each of the POR's seven high-level principles explicitly indicate their applicability to third-party arrangements. They conclude that outsourcing of services to third parties is an important factor for banks to consider when strengthening their operational resilience and that a consistent implementation of the existing third-party dependency management is essential.

In March 2022, the BCBS issued a newsletter to provide greater detail on its internal discussions regarding third- and fourth-party risk management and concentration risk.[56] As part of these discussions the BCBS conducted a series of outreach sessions with private sector participants and supervisors from various jurisdictions to assess the status of better established practices related to third-party risk management, and to exchange views regarding evolving practices related to fourth-party risk management and concentration risk matters. The outreach sessions confirmed the importance of banks implementing the principles set out in the PSMOR and POR.

Building on the insights gained from these sessions and on the work of the FSB in this area, the BCBS plans to develop updated supervisory principles on banks' outsourcing practices and reliance on third- and fourth-party service providers.

---

55 See BCBS (2021), *Revisions to the Principles for the Sound Management of Operational Risk*, March, and BCBS (2021), *Principles for Operational Resilience*, March.

56 See BCBS (2022), Newsletter on third- and fourth-party risk management and concentration risk, March.

IOSCO

Principles on Outsourcing (2021)[57]

Background: In October 2021, the IOSCO published an updated set of outsourcing principles to ensure operational resilience. The Principles on Outsourcing are based on the earlier Outsourcing Principles for Market Intermediaries and for Markets but have been updated in light of new developments in markets and technology, such as the use of cloud, ICT, data localisation and recent operational events such as COVID-19. The Principles apply to trading venues, intermediaries market participants acting on a proprietary basis and credit rating agencies. While financial market infrastructures (FMIs) are outside the scope of the Principles, FMIs may consider applying the Principles.

The revised principles comprise a set of fundamental precepts and seven principles.

The fundamental precepts cover overarching issues, namely:

1. Scope
2. The definition of outsourcing
3. Responsibility for outsourcing
4. Potential risks and challenges
5. The assessment of materiality and criticality
6. Application to affiliates
7. The treatment of sub-outsourcing and outsourcing on a cross-border basis
8. Sub-outsourcing
9. Concentration of outsourcing tasks

The seven principles set out expectations for regulated entities that outsource tasks and include guidance for implementation for each principle. The principles cover the lifecycle of an outsourcing relationship, broken down into the following areas:

1. Due diligence in the selection and monitoring of a service provider and its performance
2. The contract with a service provider
3. Information security, business resilience, continuity and disaster recovery
4. Confidentiality Issues

---

57 See IOSCO (2021), ***Principles on Outsourcing***, October.

5. Concentration of outsourcing arrangements

6. Access to data, premises, personnel and associated rights of inspection

7. Termination of outsourcing arrangements

An Annex describes how outsourcing integrates with cloud computing.

Concentration Risk: With respect to concentration, Principle 5 provides that "*A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself." But notes that "The application of this Principle and the means of implementation below should therefore apply to the extent that the regulated entity is aware or should be aware of concentration risks from many regulated entities' reliance on one or very few service providers.*"

Materiality and Criticality: With respect to the assessment of materiality and criticality, Precept D provides that "*These Principles should be applied according to the degree of materiality or criticality of the outsourced task ..and.. , the regulated entity should develop a process for determining the materiality or criticality of the tasks it is seeking to outsource…In simple terms, a material task is one that comprises or affects a significant proportion of the activities, operations, clients or market relationships and would introduce a material or unacceptable level of risk to the entity if they were to fail…An outsourced task is critical if it is critical to the functioning of the regulated entity or the integrity of financial markets. A critical task may be a task that is small in scale but without which the regulated entity is unable to conduct its activities such that the regulated entity is unable to meet its own obligations to its clients or to comply with applicable regulations.*"

Sub-Outsourcing: With respect to sub outsourcing Precept G provides that "*regulated entities should take appropriate measures if the sub-outsourcing could have material adverse effects on the outsourcing arrangement of a critical or material function or would lead to a material increase of risk. Such measures may include objecting to the sub-outsourcing, and/or terminating the contract.*"

Cyber-Risks: With respect to cyber risks under Principle 3 "*Effective, secure and resilient information technology systems are fundamental to the markets. Cyber vulnerabilities may arise through connections to unsecure vendors and the exploitation of information and communication platforms.*" and so "*Regulated entities should take appropriate steps to ensure that third parties have in place a comprehensive cyber security and resilience program.*" To that end the report follows the approach set out in the IOSCO Cyber Task Force Final Report (2019)[58] with respect to third-party providers, namely that "*To avoid overlap or duplication, the regulated entities should look to and implement existing cyber frameworks to address these risks. The Core Standards that may be applied include:*

- *CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures;*

[58] See IOSCO (2019), *Cyber Task Force Final Report*, June.

- *National Institute of Standards and Technology (NIST) Cybersecurity Framework;*
- *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27000 family of standards;*
- *G7 fundamental elements for third-party cyber risk management in the financial sector*".

Final Report on Operational resilience of trading venues and market intermediaries (2022)[59]

This IOSCO report sets out some lessons learnt on the operational resilience of trading venues and market intermediaries during the pandemic. It looks at the existing IOSCO operational resilience principles, recommendations and guidance that provide the core structure operational resilience (in particular the Reports Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (2015); Market Intermediary Business Continuity and Recovery Planning (2015), and the findings in this report suggest this framework has worked well. Some relevant points include:

Consistent Definition of Operational Resilience and Critical Functions: The Report defines *"operational resilience refers to the ability of a regulated entity to deliver critical operations through disruption*. This description of operational resilience is based on the definition of operational resilience used by the Basel Committee on Banking Supervision (BCBS) in its Principles for Operational Resilience. With respect to Critical Operations the report provides that "*Operational resilience requires extensive planning and preparation, including the identification of a regulated entity's critical operations, relationships and activities and consideration of the possible risks to its ability to deliver its critical operations. And that Critical operations encompass critical functions (see BCBS Report)* but notes *"As with the description of operational resilience, IOSCO is drawing on the BCBS's description of critical operations. However, again, while the underlying principles may be the same, the specifically identified critical operations of a regulated entity may differ from that of a bank."*

Third-Party and Offshore Vulnerabilities: One of the key lessons learnt in the Report is to "*Consider dependencies and interconnectivity – full business processes and all dependencies and interconnections are important to consider before and after a disruption to adequately assess potential risks and changes to controls. Critical to this is consideration of the role of service providers and offshore services, whether intragroup or third parties."* The report also notes that *"If a regulated entity does not assess its interconnections and dependencies, or the operations of its service providers and the service provider's business continuity and recovery plans, a regulated entity may not be able to recover or shift its operations in the face of a large-scale disruption."*

Identifying and Mapping Dependencies: *"Highlighted the importance "[i]dentify[ing] the business functions and systems that are critical to continue operations in the face of a [disruption]"*and that *"When evaluating their approaches to operational resilience, it is important for regulated entities to consider their full business process and all dependencies throughout the supply chain (both internal and external) to adequately address risks and controls. As part of this*

59 See IOSCO (2022), *Final Report on Operational resilience of trading venues and market intermediaries* , July.

process, it is important for entities to understand and map critical functions, internal and external dependencies, identify concentration risks and identify likely points of failures and options for reducing the risk."

Planning for a wider range of risks: The Report also recommended that "a *broad range of scenarios (even those that are unlikely) may be appropriate to be tested.*" and in particular, with respect to third parties *"challenges to operational resilience for all regulated entities may be symmetrical as well as asymmetrical. For instance, a future challenge may be a scenario where all service providers suffer an outage and simply moving to a different service provider or backup location may not be an option to help ensure the delivery of critical operations through a disruption. Likewise, limitations or restrictions on the ability of regulated entities to carry on services may be more widespread than anticipated or planned for by regulated entities."*

CPMI-IOSCO

Annex F of the *Principles for financial market infrastructures*[60] sets out expectations aimed at critical service providers (CSPs). It covers risk identification and management, information security, reliability and resilience, technology planning and communication with users. Although the financial market infrastructure (FMI) remains ultimately responsible for its operations, the regulator, supervisor or overseer of the FMI may use Annex F to establish expectations specifically targeted at CSPs. A number of authorities have done so, including the National Bank of Belgium for SWIFT,[61] the Bank of England and the Eurosystem.

CPMI-IOSCO has issued guidance to FMIs to enhance their cyber resilience.[62] The guidance notes that, unlike physical operational disruptions, the cyber risk posed by an interconnected entity is not necessarily related to the degree of that entity's relevance to the FMI's business. Thus, FMIs should adopt a risk-based approach to mitigating cyber risk from third parties.[63]

More recently, management of third-party services had been highlighted in two CPMI-IOSCO implementation monitoring reports.

- The 2021 assessment of business continuity planning practices[64] at 38 FMIs did not find any issues of concern regarding interdependencies with third parties. It reported that a significant majority of the FMIs stated that they have identified operational risks posed by service providers. The main types of service providers identified were financial messaging providers, outsourced data centres and application/software developers; although the latter two were not always considered to be critical. Most FMIs indicated that at least a subset of CSPs are involved in some of the FMIs' business continuity tests, and a small number of FMIs participated in the CSPs' business continuity tests.

---

60 See CPMI-IOSCO (2012), *Principles for financial market infrastructures*, April. April. Available on the CPMI and IOSCO websites.

61 The National Bank of Belgium oversees SWIFT in accordance with the "High level expectations for the oversight of SWIFT", which are aligned with Annex F.

62 See CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures (FMI), June. Available on the CPMI and IOSCO websites.

63 Paragraph 1.3.6 of the Guidance on cyber resilience for financial market infrastructures.

64 See CPMI-IOSCO (2021), Implementation monitoring of PFMI: Level 3 assessment of FMIs' business continuity planning, July. Available on the CPMI and IOSCO websites.

- The 2022 assessment of cyber resilience[65] at 37 FMIs concluded that most FMIs did not include CSPs in the testing of their response, resumption and recovery plans and processes with respect to cyber incidents. This finding calls into question the ability of such FMIs to identify, monitor and manage the risks from external parties (including CSPs), which may hinder their capacity to recover and resume operations following a cyber incident.

IAIS

The IAIS' Operational Resilience Task Force issued for public consultation an Issues Paper on Insurance Sector Operational Resilience.[66] The objective of the Issues Paper is to identify issues impacting operational resilience in the insurance sector and provide examples of how supervisors are approaching these developments, with consideration of lessons learnt during the Covid-19 pandemic. Recognising that operational resilience is a broad and evolving area, this paper addresses three specific operational resilience sub-topics concerning areas the Task Force considers as matters of significant and increasing operational risk, and therefore of immediate interest to supervisors:

- Cyber resilience;
- Third-party outsourcing; and
- Business Continuity Management.

The IAIS paper specifically discusses third-party provision of critical IT services. It observes: "*The use of advancing technologies, such as the cloud, could provide efficiencies and improvements in cyber security as compared to in-house legacy technology infrastructure and systems. However, dependencies on third parties can also magnify cyber risk.*"[67]

The paper explains that "*including third parties in cyber resilience assessments can enhance the identification of risks and the implementation of relevant risk mitigation strategies*", and suggests that "*when assessing an insurer's cyber resilience framework, supervisors may consider how dependencies on critical third-party suppliers are identified and the extent to which such dependencies create significant vulnerabilities.*"[68]

The paper is informed by a review of the IAIS Insurance Core Principles, a stocktake of existing publications by Standard Setting Bodies (SSBs) with relevance to operational resilience, direct engagement – including roundtables – held with operational resilience experts external to the IAIS membership, and information shared on supervisory practices among insurance supervisors.

---

65 See CPMI (2022), *Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience*, November.

66 See IAIS (2022), *Public Consultation on Issues Paper on Insurance Sector Operational Resilience*, October.

67 Id. at p.8, par. 27.

68 Id. at p.8, par. 28.

G7 Fundamental Elements

In October 2022, the G7 Cyber Experts Group (CEG) issued an updated set of G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector from the version issued in 2018. To address industry developments since 2018, the G7 has revised the 2018 Fundamental Elements to focus not only on the management of third-party relationships but also on ICT supply chain management. The updated Fundamental Elements stress the importance of extensive information sharing and transparency to cope with an ever-changing threat landscape. To draw attention to the increasingly important role of third parties in the financial sector, a new fundamental element has been added. Entities should tailor the Fundamental Elements, as appropriate, to their specific risk profiles, operational and threat landscapes, roles in the sector, and legal and regulatory frameworks. The elements are non-binding and do not invalidate existing frameworks or prevent their continuous adaptation. The following Fundamental Elements consider the Third-Party Cyber Risk Management Life Cycle within an individual entity, the role of a third party to the financial sector, as well as system-wide monitoring of cyber risk. Moreover, these Fundamental Elements consider the Third-Party Cyber Risk Management within the entire ICT supply chain of an individual entity.

Entities and third parties can use these Fundamental Elements as part of their cyber risk management toolkit. In doing so, entities should apply a proportionate approach that takes into account the size, nature, scope, complexity and potential systemic significance of the third-party relationship. Authorities within and across jurisdictions can use the Fundamental Elements to inform their public policy, regulatory, and supervisory efforts to address third-party cyber risks.

In June 2019, the G7 CEG delivered the first cross-border coordination exercise across the G7 (involving 23 financial supervisory authorities). Following this exercise, the G7 CEG agreed to make simulation exercises a permanent part of its mandate and developed the “G7 Fundamental Elements of Cyber Exercise Programmes” as a framework for future exercises. The G7 Fundamental Elements of Cyber Exercise Programmes are addressed to financial institutions but recognise the potential role of other stakeholders in these exercises. For instance, the planners of these exercises should “*assess their interconnections to other companies and the companies upon which they are operationally dependent, e.g., third-party service providers, often referred to as an ecosystem scan.*” Planners may also “*consider including such experts from departments representing communications, legal, business line owners, sister agencies, law enforcement, and critical third parties such as internet service providers or telecommunications in exercises.*”

In 2018, the G7 published the Fundamental Elements for Threat Led Penetration Testing Data (TLPT) to “*provide core elements of and approaches for the conduct of TLPT across G-7 jurisdictions*” and “*facilitate greater compatibility among TLPT approaches.*” Like the G7 Fundamental Elements of Cyber Exercise Programmes, the Fundamental Elements for TLPT are addressed to financial institutions but note that they “*should identify the underlying people, processes and technology supporting those critical functions and services, including third-party providers (such as IT service providers and supply chain relationships). If the test requires the inclusion of third-party providers within the scope, it is the responsibility of the entity to liaise and ensure the participation of the third-party provider.*”

Annex 2: Regimes pursuing supervision of certain critical third-party services and/or service providers

Some supervisory authorities have or are in the process of acquiring powers to supervise the provision of certain critical services by third-party service providers, such as those deemed to give rise to systemic third-party dependencies. Box 1 summarises these regimes.

Box 1: Examples of regimes

US Bank Service Company Act (BSCA)

The BSCA allows for the US Federal Banking Agencies (FBA) to supervise and regulate certain bank services provided by third parties. In particular, the BSCA provides that when an FBA-regulated bank or its affiliate causes to be performed for itself (by contract or otherwise) bank services, then the performance of the bank services is subject to regulation and examination by the FBA to the same extent as if those services were being performed by the bank. Title VIII of the Dodd-Frank Act also allows supervisory agencies of designated financial market utilities (DFMUs) – currently the FRB, SEC, and CFTC – to examine the provision of a service provided by another entity when such a service is "integral" to the operation of the DFMU.

EU Digital Operational Resilience Act (DORA)

DORA provides for the creation of an EU oversight framework for critical Information Communication Technologies (ICT) third-party service providers to EU financial entities. The European Supervisory Authorities (ESAs)[69] will designate critical ICT third-party service providers (there will also be an opt-in process for service providers to apply for voluntary designation even if they are not initially designated by the authorities). The ESAs have powers to request information, conduct investigations and inspections, issue recommendations to critical ICT third-party service providers, impose periodic penalties to critical ICT third-party service providers who failed to comply with requests for information or refused to submit to investigations and inspections, and in certain circumstances to request financial entities to suspend or terminate the contracts for the provision of services by ICT critical third-party service providers. The rules in DORA will become applicable starting 17 January 2025. The drafting of accompanying regulatory and implementing technical standards, as well as guidelines is on-going.

Proposed Critical Third Parties Regime (UK):

The Financial Services and Markets Bill that was put before the UK Parliament in July 2022 sets out the legal foundations for these measures, which would give (i) HMT powers to designate certain third-party service providers as Critical Third Parties (CTPs); and (ii) the regulators powers to make rules for, gather information from and (if appropriate) take enforcement action against CTPs. The UK supervisory authorities envisage using their proposed rulemaking powers in respect of CTPs to impose minimum requirements on the resilience of critical services they provide to the UK financial sector and set out a range of tools to test the resilience of those services (potentially in collaboration with other stakeholders, including authorities in other jurisdictions).[70]

69 The European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

70 See PRA, FCA, BOE (2022) *Operational resilience: Critical third parties to the UK financial sector*, July.

Abbreviations

BCBS	Basel Committee on Banking Supervision
BIA	Business Impact Analyses
CIR	Cyber Incident Reporting
CPMI	Committee on Payments and Market Infrastructures
CSP	Critical service provider
CTP	Critical third-party
DORA	EU Digital Operational Resilience Act
FMI	Financial market infrastructure
FSB	Financial Stability Board
G7 CEG	G7 Cyber Experts Group
IAIS	International Association of Insurance Supervisors
ICT	Information and communications technology
IOSCO	International Organization of Securities Commissions
KPI	Key Performance Indicator
MoU	Memorandum of Understanding
PSMOR	BCBS Principles for the Sound Management of Operational Risk
POR	BCBS Principles for Operational Resilience
RPO	Recovery point objective
RTO	Recovery time objective
SIFIs	Systemically Important Financial Institutions
SRC	Standing Committee on Supervisory and Regulatory Cooperation
SSB	Standard-setting body
TLPT	Threat Led Penetration Testing