Proposed GFMA principles regarding Critical Third Parties

June 2022

I. Background

- Financial Institutions (FIs) are only one part of the financial services ecosystem. Some third-party providers (TPPs) that sit outside of the financial services regulatory perimeter are playing an increasingly important role in the financial system. In many cases, TPPs perform critical activities for FIs and operate in highly concentrated sectors.
- Global authorities and regulators are increasingly assessing the risks posed by these critical third parties (CTPs) (including Cloud Service Providers (CSPs)) and the potential impact on financial stability. This is apparent from recent announcements (UK FPC and HM Treasury), speeches (BIS), and other more concrete developments (EU, Korea, MAS, FSB). At the core of authorities' concerns is the possibility that a concentration of services in a small number of TPPs may mean that a failure or disruption, whether technical, commercial, or legal, at one or more of those providers could impact the provision of financial services so severely that it leads to a financial stability event. While the major CSPs are the main use case for this concern, authorities are also considering other IT TPPs, which, while less prominent, could represent a single point of failure.
- This is still an emerging topic at an early stage of debate and with many options being considered. This GFMA paper, therefore, outlines our set of proposed principles on how to best address these risks and is looking to proactively engage with regulators and standard setters on this important topic.

II. Proposed GFMA Principles regarding Critical Third Parties

Principle 1: Authorities should focus on risks to systemic financial stability and enabling greater recovery capability

1. The financial industry is well-regulated and is subject to longstanding outsourcing, third-party risk management, and technology risk management rules, regulations and guidelines[1]. As part of their own risk management frameworks, FIs have well-established third-party risk management controls in place to mitigate the risks relating to outsourcing and third-party relationships, including cybersecurity, information technology, data privacy and concentration.
2. In considering the need for any additional regulatory action, authorities therefore should focus on **addressing potential risks to systemic financial stability** arising from the financial industry's reliance on a concentrated set of CTPs that are not already addressed under existing regulatory regimes.
3. Concentration in itself is not inherently bad and can generate certain advantages, including reduced complexity and easier management and control of a smaller number of parties. However, we recognize that dependencies due to concentration can put the stability of the financial system at risk in the event of a major failure. While FIs generally already assess and address their own third-party concentration risk as part of their ongoing operational resilience, they are unable to assess accurately the risk posed to systemic financial

[1] e.g. for Asia, see annex I of https://www.asifma.org/wp-content/uploads/2018/07/leading-principles-for-regulation-of-outsourcing.pdf; for Europe, see schedules 4 & 5 of https://www.afme.eu/publications/reports/details/Outsourcing---Guidance-on-the-Legal-and-Regulatory-Framework; for US, see https://www.sifma.org/resources/general/third-party-risk-management/ -

stability. This can only be undertaken by regulators, in close consultation with FIs and CTPs, the latter of whom become increasingly important when 4th/5th/nth parties are involved.

4. **In particular, the focus should be on the risk of major and prolonged outage(s):** authorities should aim to reduce the length and impact of any outages and improve recovery from major outages. It should be acknowledged that there will be failures and incidents, and authorities should therefore not focus on preventing every single outage as this would be unrealistic and disproportionate. Efforts should be focused on minimising the possibility of a major and prolonged outage and mitigating its potential consequences. This would mean that, in addition to good preventative security controls (e.g., a change management programme), additional oversight measures of CTPs should be primarily concerned with recovery and restoration capabilities of the CTPs along with incident management and communication measures.
5. **Participation in resilience exercises:** Regulators can also help bring together FIs and CTPs in industry resilience exercises to evaluate how real-world scenarios would impact operations and recovery, which has already proven useful in some jurisdictions and at the global level, for example the GFMA Quantum Dawn[2] exercises, the UK-US System Integrity Reconnection Exercise and the U.S. Treasury OCCIP Hamilton tabletop CSP Exercise for large FIs. Such exercises and testing would allow all concerned parties to better understand roles and responsibilities, identify any potential gaps in these relationships, increase collaboration and ultimately strengthen the resilience of the overall system.

<u>Principle 2: Strengthen financial stability by enabling greater innovation and competition, not erecting barriers</u>

1. If required, further regulatory action should be **principles-based and focus on the desired outcomes (e.g., ultimately the need to maintain financial stability)** in order to avoid inhibiting digitisation and innovation. CTPs play a critical role empowering FIs to innovate and modernize legacy systems with the offering of a world class technology stack and security. Therefore, any further regulatory intervention should balance the need to manage financial stability risk against the possibility of eventually deterring CTPs from conducting business with or limiting their services offering to the financial sector.
2. **Support greater competition:** Authorities should adopt approaches that encourage greater competition among CTPs, recognising that over time this will reduce concentration and encourage innovation. In any event, their actions should not impede or inhibit competition.
    a. In the context of the CTP oversight regimes currently proposed, authorities should consider explicitly the impact their proposals will have on FIs' access to third-party suppliers. It should be recognised that it is unlikely that suppliers of the financial services market will be diversified to such an extent that there will not be some level of concentration risk.
    b. Being designated as a CTP could be interpreted by FIs as a 'mark of quality' due to a belief that CTPs would pose an ongoing lower risk than non-designated TPPs. This could lead to greater concentration. Authorities should be clear that direct oversight/supervision is a reflection of the provider's systemic relevance and does not indicate a preference over non-designated TPPs.
    c. At the same time, actions taken by authorities to reduce concentration in CTPs should be carefully considered to avoid limiting disproportionally FIs' ability to make use of certain providers, for instance through prescriptive requirements such as exposure limits or forced rotation as these rules could contribute to further concentration or decreased resilience.

<u>Principle 3: Increase collaboration across borders, sectors, regulators and all relevant stakeholders</u>

[2] GFMA: https://www.sifma.org/resources/general/fact-sheet-quantum-dawn-6/

1. **International collaboration:** Collaboration and harmonisation of approaches is needed at a global level. Given the cross-border and often global operations of CTPs and the nature of the financial system, coordination amongst authorities, including international standard-setting bodies such as the financial stability board (FSB), the International Organisations of Securities Commissions (IOSCO) and the Bank for International Settlements (BIS), is necessary to minimise fragmentation of FIs' technology operations and avoid the emergence of additional IT risk by increasing complexity. Unilateral, uncoordinated approaches could decrease, rather than increase, the operational resilience of the global financial system. Consistent understanding at the international level of existing regulatory obligations for third-party relationships would strengthen FIs' ability to manage risks. One example is the definition of "materiality", the understanding of which differs across jurisdictions, creating difficulties for the global governance of third-party risks.
2. **Cross-sectoral approach:** A cross-sectoral approach with authorities is also needed involving other relevant government authorities alongside financial regulators such as competition authorities, data protection authorities, financial authorities, cybersecurity agencies, etc., to ensure that consistent and complementary requirements support shared goals rather than distract, duplicate or conflict.
3. **Collaboration between public sector, regulatory authorities, financial sector and CTPs** is needed to improve common understanding and bridge knowledge gaps (e.g., through joint stress testing efforts for example as mentioned in principle 1.5 above).
4. **Operationalising existing rules:** To better address financial stability risk stemming from the concentration of CTPs, we suggest a more coordinated approach focusing on increasing transparency of and access to necessary information for customers of CTPs which in turn will support resilience by improving information flows.

<u>Principle 4: Avoid approaches which drive fragmentation and may exacerbate financial stability risk</u>

1. **Avoid localisation:** Fragmentation of FIs' operations or the localisation of a CTP's services is detrimental to FIs' security and resilience and should be avoided.
    a. Authorities should avoid any requirement which prevents FIs from engaging the services of a CTP located outside of the supervisor's jurisdiction. Such requirements could result in significant fragmentation in FIs' operations thereby undermining rather than strengthening the security and resilience of the sector.
    b. Localisation may also increase market concentration and dependencies as certain CTPs may choose to invest in infrastructure only in certain jurisdictions, reducing local offering and contributing to a degree of vendor lock-in for FIs operating in that market.
    c. We urge authorities to work constructively with each other on enabling frameworks for cross-border data flows, such as for example the Singapore-US Joint Statement on Financial Services Data Connectivity[3],the Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas (BSP) and The Monetary Authority of Singapore[4], and the Singapore-UK Digital Economy Agreement[5].

[3] MAS, 2020: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

[4] MAS, 2020: https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas#:~:text=16%20November%202020-,Joint%20Statement%20of%20Intent%20on%20Data%20Connectivity%20between%20Bangko%20Sentral,The%20Monetary%20Authority%20of%20Singapore&text=1.1.,development%20of%20the%20financial%20sector.

[5] Ministry of Trade and Industry Singapore, 2022: https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/UKSDEA

2. **Avoid ring-fencing:** CTPs should not be forced to ringfence the services they provide to FIs (e.g., financial services cloud should be avoided)
    a. Although the use of separate infrastructure may make it easier to demand certain requirements of the service being provided, it does not in itself lead to resilience benefits and comes at great cost.[6]
    b. Ring-fenced services (for instances within a CSP) often offer inferior capabilities and often prevent users from being able to make use of the latest product offerings, including those which improve security and resilience.
    c. Such limitations may also negatively impact the competitiveness of FIs.
    d. Ringfencing potentially creates a single point of failure and a more attractive target for adversaries, insider threats and increases concentration risks.

3. Avoid forced multi-vendor strategies and forced termination of contracts
    a. We suggest there should be minimum regulatory interference in FIs' own third-party strategies (e.g., multi cloud, hybrid, type of provider, etc.), including how they choose to contract with CTPs. Such decisions should instead be driven by distinct features that will be unique to each individual FI – e.g., their overall business strategy, risk profile, footprint etc.
    b. Multi-cloud strategies, while often used for contingency and resilience, are primarily adopted for accessing unique services across CSPs. While multi-cloud can reduce concentration risk to some extent, the technical, process and resource complexity needed to support multiple CSPs can lead to decreased resilience overall. A multi-cloud approach can create challenges, such as increased costs, technical complexity, and additional specialist skillsets required to onboard and manage multiple CSPs.[7]
    c. Given the disruptive operational impact of forced contract termination, this power should only be considered as a last resort measure, in close collaboration with the concerned FI and with considerable advanced planning. We suggest that any enhanced oversight of CTPs by authorities should steer away from creating new rules in relation to forced termination of the contractual relationship between the FI and the CTP.
    d. Authorities should also not attempt to mandate the legal structure or location of any contractual agreement between the FI and CTP. Doing so is likely to limit choices of CTPs for FIs and could indirectly lead to creating more concentration. It could also make it more difficult to achieve the concessions needed to meet the FI's regulatory requirements.

<u>Principle 5: Data access responsibilities should be clearly defined and requests directed to the data owner</u>

It is important to clarify how FI's data stored by CTPs or data pertaining to CTPs will be accessed by financial regulators.

1. **FI data:** regulation requires FIs to maintain supervisory access terms in their contracts with CTPs to access data relevant to the FIs for their own risk assessments and to provide this information to financial regulators as required a. However, while financial authorities should continue to leverage these existing powers, they should also recognise that there are often contractual limitations to gathering data to assess risks related to CTP subcontractors, particularly from the 5th party onwards.
2. **CTP data:** data which is relevant to the operations of the CTP and to assess concentration and supply chain risk should be directly accessed by regulators from CTPs. This should include assessments of CTP subcontractors where FIs find it difficult to acquire the appropriate data. This will enable authorities to

[6] Atlantic Council, Four Myths About The Cloud: the geopolitics of cloud computing, p.19. https://www.atlanticcouncil.org/wp-content/uploads/2020/09/CLOUD-MYTHS-REPORT.pdf

[7] https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_CloudComputing2021_06-2.pdf

better assess concentration risks posed to both individual FI stability and systemic financial stability, in particular by building a better understanding of how critical 5th/nth parties themselves are to the operational resilience of CTPs and the services they provide.

ANNEX: AFME/ASIFMA/SIFMA work on public cloud

The GFMA tri-trades have all been working with members on the issue of cloud benefits/regs and/or recommendations for regulatory approaches.

- ASIFMA published in March 2021 Proposed Principles for Public Cloud Regulation and has been engaging with key Asian regulators on the back of the launch of these principles
- AFME published in September 2021 a paper on Building Resilience in the Cloud
- SIFMA published in October 2020 a paper on Navigating Regulatory Challenges in Cloud Infrastructure Services Agreements