WASHINGTON, DC • LONDON • BRUSSELS • HONG KONG • WWW.ICI.ORG

August 21, 2023

Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland
Submitted electronically to: fsb@fsb.org

Re: *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*

Dear Sir/Madam:

The Investment Company Institute (ICI), including ICI Global,[1] appreciates the opportunity to provide feedback to the Financial Stability Board (FSB) on its consultation, *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*.[2] ICI's mission is to strengthen the foundation of the asset management industry for the ultimate benefit of the long-term individual investor. Our members invest on behalf of millions of retail investors around the world who choose investment funds to save for retirement, education, and other important financial goals.

We provide comments on the consultation from the perspective of asset managers and the investment products they offer and manage for long-term investors, which may be subject to different regulatory requirements and have different kinds of third-party arrangements than other types of financial institutions, such as banks and insurance companies.

We generally support the overall goals and approach of the FSB's consultation and its use of a toolkit, rather than recommendations. We would be concerned, however, if the tools in the toolkit were treated as recommendations that jurisdictions should mandate. We, therefore, request that the FSB make clear in its final report that the toolkit is an *optional* reference resource that financial institutions and financial authorities may use in developing and

[1] The Investment Company Institute (ICI) is the leading association representing regulated investment funds. ICI's mission is to strengthen the foundation of the asset management industry for the ultimate benefit of the long-term individual investor. ICI's members include mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and UCITS and similar funds offered to investors in other jurisdictions. Its members manage $31.2 trillion invested in funds registered under the US Investment Company Act of 1940, serving more than 100 million investors. Members manage an additional $8.7 trillion in regulated fund assets managed outside the United States. ICI also represents its members in their capacity as investment advisers to certain collective investment trusts (CITs) and retail separately managed accounts (SMAs). ICI has offices in Washington DC, Brussels, London, and Hong Kong and carries out its international work through ICI Global.

[2] FSB, *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities* (June 2023), available at https://www.fsb.org/wp-content/uploads/P220623.pdf.

implementing their own approaches and that the intent is not for financial authorities to require the use of any tool in the toolkit.

I. ICI Supports the Overall Goals of the Toolkit

We support the development of the toolkit, with the goals of:

1) reducing fragmentation in regulatory and supervisory approaches to financial institutions' third-party risk management across jurisdictions and different areas of the financial services sector;
2) strengthening financial institutions' ability to manage third-party risks and financial authorities' ability to monitor and strengthen the resilience of the financial system; and
3) facilitating coordination among relevant stakeholders (i.e. financial authorities, financial institutions and third-party service providers).

We also support the efforts to promote interoperability of approaches and the principle of proportionality. We agree that the toolkit should not promote a one-size-fits-all approach. Importantly, the consultation recognizes that risks differ between jurisdictions and regions and across different areas of the financial services sector. Indeed, third-party service provider risks for the asset management sector may differ from those of the banking and insurance sectors and, even within the asset management sector, the use of third-party service providers and the level of their criticality to services can vary significantly across asset managers and investment products.

We also welcome the FSB's work on developing an optional toolkit that financial institutions might reference when developing and implementing their own third-party service provider risk management processes and that financial authorities might reference in connection with their supervisory responsibilities. We support the toolkit as long as it is treated as an *optional* reference resource and not treated as recommendations that jurisdictions should mandate the tools' use. We believe this is consistent with the FSB's intent. Nevertheless, some references in the discussion of the toolkit for financial authorities could be clarified to avoid this misinterpretation, as we discuss in Section II below.

A. Tools for Financial Institutions

We generally agree that the tools for financial institutions provide useful tips for management of third-party critical service provider risks. Many of the tools listed, including for the identification of critical services and onboarding and ongoing monitoring of service providers, are often used by asset managers. It is a common business practice for asset managers to conduct appropriate due diligence prior to commencing an engagement with a third-party service provider and to enter into written agreements with them prior to retaining their services. Further, after conducting due diligence into a service provider and establishing a relationship pursuant to a written agreement, asset managers routinely monitor the service provider's activities and performance. Because different jurisdictions have different regulatory approaches, however, it is important that the toolkit is clearly presented as optional. For example, in the United States, investment advisers are subject to a fiduciary duty and required to oversee outsourced service providers in accordance with that duty whereas other countries have decided to adopt regulations and codify outsourcing oversight requirements. Given the difference in regulatory approaches and requirements, not every "tool" in the toolkit can be, nor should be, uniformly adopted by every asset manager in every jurisdiction.

Moreover, asset managers generally assess the risks of the service providers to the manager so that their oversight and allocation of resources is proportional to the risk. Asset managers may not necessarily maintain "registers" and all the accompanying information the consultation contemplates, however. In the US, for example, common business practices do not generally include the use of such registers. In addition, as we discuss below, any such lists obtained by financial authorities, as well as information from incident reports, must be highly protected and the use of the information by authorities should be highly restricted. Depending on the cybersecurity controls of the relevant financial authority, submitting such sensitive information might not represent a common business practice.

Regarding management of risks from service providers' supply chains, we appreciate the consultation report's acknowledgement that it can be impractical to directly assess and manage every unique risk across each element of a third-party service provider's supply chains. We agree that the toolkit should be applied in a proportionate and risk-based manner.

B. Tools for Financial Authorities

In addition to tools for financial institutions, the consultation includes tools for financial authorities. We are generally supportive of the toolkit as an optional reference resource but have some suggestions for clarifying its application.

The tools for financial authorities are intended to help them in: (1) supervising how financial institutions manage third-party risks, and (2) identifying and monitoring systemic third-party dependencies, and potential systemic risks and managing those risks.

Regarding the first prong, we note that not all financial authorities have adopted specified measures to supervise how a financial institution manages third-party risks and may not have the authority to do so. For example, under current US federal securities laws,[3] an investment adviser oversees outsourced functions consistent with its fiduciary duty and other legal obligations, which is a very flexible approach with little codification.[4] While other jurisdictions may have adopted regulations to varying degrees for some entities and with different areas of focus, not every jurisdiction has adopted measures for every financial entity that prescribe oversight for every utilized service provider, particularly as it relates to service providers that do not constitute outsourced arrangements.[5] Therefore, the toolkit should not presume that financial authorities have prescriptive authority or the desire to implement

---

[3] On October 26, 2022, the US Securities and Exchange Commission (SEC) issued a proposal that included a prescriptive rule governing oversight by investment advisers of outsourced service providers. *See Outsourcing by Investment Advisers*, 87 Fed. Reg. 68816 (Nov. 16, 2022), *available at* https://www.govinfo.gov/content/pkg/FR-2022-11-16/pdf/2022-23694.pdf. This proposal has not been adopted, and the comments submitted in response to this proposal were overwhelmingly negative and generally in line with ICI's letter, which outright opposed the proposal. *See* ICI Letter to SEC regarding *Outsourcing by Investment Advisers* (December 23, 2022), *available at* https://www.ici.org/system/files/2022-12/22-ici-cl-sec-outsourcing-by-inv-adv.pdf. Consistent with that letter, ICI again reiterates its opposition to any prescriptive approach to oversight of service providers.

[4] The SEC has the authority to bring enforcement cases for failure to adequately oversee service providers, however, when the failure to oversee constitutes a breach of fiduciary duty based on the totality of the facts and circumstances. *See* In the Matter of Aegon USA Investment Management, LLC, et al., Advisers Act Release No. 4996 (Aug. 27, 2018) (settled order) (adviser utilizing third-party models without first confirming that the models worked as intended); Morgan Stanley Smith Barney LLC, Advisers Act Release No. 6138 (Sept. 20, 2022) (settled order) (adviser failing to oversee a third-party vendor that did not properly safeguard customers' personal identifying information).

[5] *E.g.* FCA Handbook SYSC 8.1; EBA Guidelines on Outsourcing Arrangements (Feb. 25, 2019).

specified measures that directly regulate how a financial institution manages third-party risks.[6]

Regarding the second prong, we appreciate that a financial authority's work depends on having access to information and data to help it identify and monitor systemic third-party dependencies and potential systemic risks. As the consultation acknowledges, only a small number of jurisdictions have powers to directly oversee the provision of services to financial institutions by critical service providers. This means that the remaining jurisdictions must rely on other ways to gather information, including through financial institutions.

The toolkit suggests that some of the information financial authorities have about service providers may come from incident reporting by financial institutions or through their registers of service providers. Due to the highly sensitive nature of this information, we recommend that the FSB emphasize the importance of adequately securing this information, including in any cross-border information sharing. For example, as we previously noted in our comments to the FSB's consultation on *Achieving Greater Convergence in Cyber Incident Reporting*,[7] if a financial institution's network is potentially compromised, incident reporting should take place through an "out of band" channel or network.

Similarly, as we indicated in our comment letter to the SEC in response to its proposal on *Outsourcing by Investment Advisers*,[8] service provider lists can be highly sensitive information that should also be appropriately protected. The SEC had proposed that investment advisers publicly disclose their service providers, which we cautioned would give hackers and other bad actors a government-funded database to enable them to target their efforts when seeking to attack asset management infrastructure systems. Although the FSB's consultation does not contemplate such public disclosure of this information, it does contemplate the maintenance of registers by financial institutions and the ability of financial authorities to access them.

We appreciate that this information can help financial authorities to identify dependencies and concentration risk, among other things, but it could also help bad actors do the same if the data and information are not appropriately protected. Incident reports and information about the use of third-party service providers should likewise be adequately protected in any cross-border information sharing. We suggest that the FSB emphasize the sensitive nature of this information and that it should be adequately secured.

---

[6] It is worth noting that when the US banking regulators, the Federal Reserve, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, opined on third-party relationships recently, they did so in the form of guidance as opposed to any prescriptive rulemaking. *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37920 (June 9, 2023), *available at* https://www.occ.gov/news-issuances/federal-register/2023/88fr37920.pdf.

[7] See ICI Letter to FSB regarding *Achieving Greater Convergence in Cyber Incident Reporting* (December 22, 2022), available at https://www.ici.org/system/files/2022-12/22-ici-cl-fsb-cyber-incident-reporting.pdf. Our comments in that letter can be incorporate into our response to this consultation as well.

[8] See ICI Letter to SEC regarding *Outsourcing by Investment Advisers*, *supra* n. 3.

II. The FSB Should Clarify it is Not Recommending Financial Authorities to Mandate a Financial Institution's Use of any Tool

As previously noted, we would be concerned if the FSB's final report were interpreted as recommendations that regulatory authorities mandate that asset managers adopt a particular tool. We appreciate that in many jurisdictions, financial authorities do not have direct supervisory authority over certain third-party service providers, but that does not mean they should achieve this authority *indirectly* by prescribing certain duties for asset managers.

The consultation states that, where financial authorities do not have the power to directly oversee the service providers, they "rely solely on the tools" for financial institutions referenced in Chapter 3 of the consultation. We recommend that the FSB make clear that not all of the tools listed in Chapter 3 may be available to financial authorities, because not all financial institutions will adopt all of the tools. Certain tools may not be appropriate for a financial institution, may not be appropriate for a given jurisdiction, or the financial institution may be able to address risk management concerns through other means not mentioned in the toolkit.

In discussing the tools for financial authorities to identify and manage potential systemic risks, such as a dialogue among authorities, financial institutions, and service providers, as well as sector-wide exercises and incident response coordination frameworks, the consultation states that these could be adopted through, among other things, requirements or expectations on financial institutions, which could reflect their arrangements with relevant third-party service providers. As discussed above, we recommend that the FSB make clear in its final report that the toolkit is not a recommendation that jurisdictions impose additional requirements or expectations on financial institutions; rather, the toolkit is an *optional* reference resource that financial institutions and financial authorities may use in developing and implementing their own approaches.

* * *

We appreciate the opportunity to provide feedback on this issue. If you have any questions regarding our response, please contact Michael N. Pedroni at +1-202-876-5352 or michael.pedroni@ici.org or Annette Capretta at +1-202-371-5436 or acapretta@ici.org.

Sincerely,

/s/ Annette Capretta

Annette Capretta
Chief Counsel, ICI Global