

November 2, 2017

Pengarah
Jabatan Dasar Kewangan Pruden
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur

Via e-mail: pfpcconsult@bnm.gov.my

Dear Sir or Madam:

The Securities Industry and Financial Markets Association (SIFMA)ⁱ and Asia Securities Industry & Financial Markets Associationⁱⁱ appreciate the opportunity to respond to the Bank Negara Malaysia's (BNM's or the Bank's) exposure draft of proposed regulatory requirements on outsourcing arrangements by financial institutions. We also thank the BNM team for graciously granting us an extension by which to submit this consultation response. Outsourcing arrangements provide important services to financial institutions, enabling them to lower operational costs that, in turn, allows them to enter and expand in the Malaysian market. We hope that the outsourcing exposure requirements will be implemented in a way that supports cross-border trade and investment, while mitigating operational and financial stability risks.

While we broadly support the objectives that the BNM is trying to achieve, we have several suggestions to improve upon the current proposal. For instance, we are concerned that the proposed pre-approval process does not include detailed principles or criteria by which BNM will grant approval for outsourcing arrangements. This introduces uncertainty in the investment climate in Malaysia for service providers and financial institutions, and will likely result in a backlog of approvals. To avoid these outcomes, we instead suggest using materiality thresholds and encourage adoption of vendor risk management frameworks whereby only material outsourced arrangements would be subject to BNM's approval process. Further, we are concerned that the proposed "transitioning arrangements" do not include transparency principles or criteria by which BNM will determine appropriate transition measures. We expand on these suggestions below.

We note that BNM has imposed a moratorium on outsourcing systems, applications and processes on foreign banks since 2013, and that these new outsourcing requirements aim to go into effect 1 January 2018. Although not specifically mentioned in the consultation paper, we are concerned that the implementation of the outsourcing guidelines in Malaysia may result in a *de-facto* on-shoring mandate. Outsourcing arrangements are critical to improving the efficiency of the financial services industry, enabling firms to provide stellar customer service, maintain competitiveness internationally, and reduce operational costs to boost investments in other areas that deepen local capital markets. We strongly

encourage the Bank Negara Malaysia to continue to recognize the importance of outsourcing arrangements to our sector, and to adopt pragmatic policies to address potential risks from third-party service providers while enabling the efficiencies that they provide. We provide additional detailed responses to the consultation questions below.

Interpretation

Question 1

Please list the arrangements that the Bank should consider to scope out from this policy document.

We appreciate the list of outsourcing arrangements that are not in scope for the draft outsourcing exposure guidelines, and suggest BNM broaden the list of arrangements scoped out of the guidelines to include:

- centralized functions without access to customers' data;
- cybersecurity and intelligence services;
- non-core banking activities;
- intra-group outsourcing arrangements;
- customer information that is encrypted securely, anonymized, or aggregated such that the identities cannot be readily inferred;
- group reporting/oversight functions where the group/affiliates are regulated entities by an authority equivalent to BNM;
- risk and control functions set up by the group;
- ad hoc load balancing activities supported by affiliate entities due to unexpected manpower shortage;
- internal employee support such as system access admin and technology and application support helpdesk;
- internal/external legal advice;
- data discovery services for litigation or potential litigation cases; and
- technology infrastructure or components that do not have end-user business access.

Policy Requirements

Question 2

Please detail out specific challenges your institution may face in meeting the requirements in paragraph 8.

We believe that financial institutions will face significant challenges to implementing the outsourcing guidance, as proposed. We suggest using materiality thresholds and encourage adoption of vendor risk

management frameworks whereby only material outsourced arrangements (whether new or renewed) would be subject to BNM's approval process.

In addition, noting the Bank's intended responsibilities for the board and senior management for outsourcing arrangements, we seek clarity on the following:

- Item 8.3: Should all outsourcing arrangements be subject to board and subsequently BNM approval? If not, what is the applicability criteria? Is the criteria the same for new and renewed outsourcing arrangements?
- Item 8.7: Is the annual assessment required for all types of outsourcing arrangements?

Risk Management

Question 3

(a) Please describe the due diligence process currently undertaken, including the considerations applied, in considering a new outsourcing arrangement as well as for the renewal or renegotiation of an existing arrangement.

(b) Where there are differences in due diligence process applied to a new and an existing arrangement, what are the operational challenges that may arise in adopting similar due diligence process for both potential and existing service providers?

N/A – As we are a trade association, we do not have details on due diligence processes to share.

Question 4

(a) Please identify any potential operational challenges in implementing the requirement in paragraph 9.8.

(b) The Bank is also considering specifying a maximum period for outsourcing agreements (i.e. 3 years). Do you agree with the proposal and the proposed duration?

The requirement for legal opinions to support an application (in paragraph 9.8) would place an undue operational burden on obtaining approvals for outsourcing. We suggest removing the requirement for legal opinions, and instead put in place an annual audit/affirmation process (without the need for a legal opinion) to comply with the guidelines. Financial institutions would generally have in place a standard template agreement to be adopted and cleared by their legal teams, with pertinent clauses incorporated in the template.

There are several challenges posed by the proposed three-year maximum term for outsourcing arrangements. Service providers have to invest in infrastructure, hardware, software, etc. that may not pass a cost-benefit analysis if the useful life of such expenditures is reduced so significantly. If service

providers are not able to secure a longer duration of contracts, they will be deterred from entering into an outsourcing arrangement. Service providers would also have to significantly increase fees to financial institutions to recover investment expenditures plus profits in this limited three-year time horizon. We suggest eliminating the proposed maximum time period for outsourcing arrangements, as firms have their own in-house outsourcing frameworks and internal audits that are sufficiently robust without the need for timeboxing.

Further, we seek clarification from BNM with regard to the following:

- Item 9.3: For outsourcing arrangements with less than one-year timeframe (if there are such), are re-assessments required upon renewal even if previous exercise was completed within the calendar year?
- Item 9.4.b: Are there any specific IT Security Controls that need to be included in the due diligence process other than incident response/management?

Question 5

Please describe measures taken by your institution to ensure that the service provider observes the confidentiality requirements, in particular once the outsourcing arrangement ceases or is terminated.

We seek clarity from the Bank on the following:

- Item 9.13: Is BNM prescribing any specific security incident notification requirements (timeline, format, etc.) between the service provider and the financial institution?
- Item 9.18.c: What constitutes acceptable physical or logical [sic] information segregation? We propose amending this requirement to state that “information must be physically or logically segregated, where reasonably practicable.”

Financial institutions recognize that they must provide appropriate, timely data to regulators upon request for them to perform their regulatory and supervisory roles, even if such documents are in the custody of the firm’s service provider. Yet there may be confidentiality requirements that inhibit service providers from meeting the requirements stipulated in paragraph 9.14, whereby service providers must allow access to systems and information to financial institutions or external auditors. As such, we suggest amending the requirement to require service providers to provide such access to information, documents and systems “where practicable.”

In addition, the requirement that financial institutions impose the same terms/requirements to sub-contractors (paragraph 9.15) is impractical. Financial institutions are not in the position to impose similar conditions since they are not a party to the sub-contracting agreement.

We also suggest amending the proposed requirement that confidentiality obligations remain in place even after the outsourcing arrangement is ceased. In our view, confidentiality obligations should cease when the data is returned, permanently destroyed, or when the data no longer remains confidential.

Question 6

Please describe your institution's current practice on BCP testing with the service provider, including the frequency of testing.

N/A – As we are a trade association, we do not have details on current BCP testing practices to share.

The requirement stipulated in paragraph 9.21, that financial institutions must have “in their possession, at all times, or can readily access” all records and information with respect to the outsourced activity implies that the activities are conducted by the financial institutions, as opposed to outsourced entities. We suggest amending this phrase to remove “has in its possession,” as well as remove “to allow it to operate.”

We note that the requirement to participate in “joint testing” is impractical from an industry standpoint. Instead, financial institutions should have access to the provider BCP tests periodically and should be able to make assessments of adequacy from them.

Regulatory Process

We encourage the BNM to consider the materiality of the outsourced activity to a firm's ongoing business activities and its ability to fulfill its regulatory obligations in its consideration of outsourcing arrangements. We seek further detail and clarity from the BNM regarding the criteria that will be used to consider and provide written approval for all new outsourcing arrangements, and renewal of existing outsourcing arrangements. It is also uncertain whether the Bank's written approval is required before negotiations of a renewal or only prior to signing the renewal contract. What is the timeline for consideration and approval of these outsourcing arrangements? We are concerned that the proposed approval process would, in practice, result in prolonged delays and leave financial institutions and their service providers in a state of uncertainty. Such delays in the approval pipeline would have adverse impacts on the ongoing operations of firms.

To avoid these outcomes, we have several suggestions for BNM. First, we encourage the Bank to set out clear expectations on the length of time that it will require to review and opine on proposed new or renewal of existing outsourcing arrangements. Second, we suggest that BNM consider the materiality of an outsourcing arrangement in determining whether prior approval would be necessary from BNM, and that other less material arrangements could be instead subject to a prior notification. We believe that changes to subcontractors should not automatically be considered “material,” particularly where such



subcontractor is not a material service provider to the outsourcing arrangement. Third, we encourage BNM to clarify the grace period that will be allowed in the event that approvals are not granted in a timely manner for the renewal of existing outsourcing arrangements. Finally, we encourage adoption of a vendor risk management framework that will allow a financial institution to assess outsourcing arrangements in accordance with this framework.

We note the required information to be provided to BNM for its consideration of outsourcing arrangements in paragraph 11.1. Instead of the remuneration of individual employees of the service provider, we propose providing the charges assessed under the outsourcing arrangement, which we believe would be more relevant and practical to implement.

Again, we thank the Bank Negara Malaysia for providing the opportunity to comment on the proposed outsourcing exposure guidelines. Yet we reiterate our serious concerns that the implementation of these outsourcing guidelines may result in a *de-facto* on-shoring mandate to the detriment of the investment climate of Malaysia. We welcome opportunities to further support the Bank Negara Malaysia's efforts to improve data confidentiality and security, as well as financial safety and soundness, while ensuring multinational financial institutions can implement the guidelines in a global operating environment. Please feel free to contact Peter Matheson (pmatheson@sifma.org or +1 202-962-7324) should you desire additional information.

Sincerely,

Kenneth E. Bentsen, Jr.
President and CEO
SIFMA

Mark Austen
CEO
ASIFMA

ⁱ SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over \$2.5 trillion for businesses and municipalities in the U.S., serving clients with over \$18.5 trillion in assets and managing more than \$67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

ⁱⁱ ASIFMA is an independent, regional trade association with over 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to



promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the [GFMA](#) alliance with [SIFMA](#) in the United States and [AFME](#) in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.