THE INVESTMENT ASSOCIATION

Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 Basel
Switzerland

The Investment Association
Camomile Court, 23 Camomile Street,
London, EC3A 7LL

+44 20 7831 0898
john.allan@theia.org
theia.org
@InvAssoc @The Investment Association

Submitted via webform

6 November 2020

Dear Sirs

RE: Consultation on Principles for Operational Resilience

The Investment Association (IA) welcomes the opportunity to comment on these proposals.

We wholly support the Committee's commitment to international engagement and collaboration on this important subject. As operational resilience is a topic that crosses all jurisdictions, together with the fact that firms face a complex global threat landscape, we believe it is important to ensure there is global regulatory alignment as far as possible. While the majority of our members will not be directly in scope of these Principles, we are seeking international cohesion on this topic.

We hope that this feedback is useful and would welcome further involvement in future discussions on this subject.

Yours faithfully,

JA

John Allan
Senior Operations Specialist

IA Response to Principles for Operational Resilience

About the Investment Association

The Investment Association (IA) champions UK investment management, a world-leading industry which helps millions of households save for the future while supporting businesses and economic growth in the UK and abroad. Our 250 members range from smaller, specialist UK firms to European and global investment managers with a UK base. Collectively, they manage £8.5trillion for savers and institutions, such as pension schemes and insurance companies, in the UK and beyond. 43% of this is for overseas customers. The UK asset management industry is the largest in Europe and the second largest globally.

Some of the IA's members are part of banking entities.

Executive summary

We welcome BCBS' commitment to international engagement and collaboration on this important subject. As operational resilience is a topic that crosses all jurisdictions, together with the fact that firms face a complex global threat landscape, we believe it is important to ensure there is global regulatory alignment as far as possible. Ensuring that the operational resilience principles are understood globally will help build trust across the financial services ecosystem that will be critical for the cross-border provision of services on which consumers rely. Moreover, international cohesion drives down compliance costs for firms and frees up resource to implement effective operational resilience strategies.

Our response focuses on some of the differences in the principles between the Committee and the UK regulators. We welcome the Committee's commitment to promote cross-jurisdictional collaboration and international engagement on this subject and in particular its principles-based nature which allows financial institutions to apply these in a proportionate manner.

Our members are well advanced on preparing for the UK authorities' new regime, and in this respect it is pleasing to see a great deal of similarity in the two approaches, such as requiring firms to understand what they do and who it is important to; understand how the firm delivers these functions; be able to measure themselves against pre-set standards; and continually test their ongoing effectiveness.

The main difference appears to be in the UK's explicit focus on the end consumer of the service or function, something that for FCA-regulated firms is a very key consideration given the regulator's consumer protection objectives. This focus then drives the requirement for impact tolerances to be set using a threshold of 'intolerable harm'. UK firms will now want to consider areas such as this in which there are differences in regulatory approaches and how it affects their work.

Answers to selected questions

1. **Has the Committee appropriately captured the necessary requirements of an effective operational resilience approach for banks? Are there any aspects that the Committee could consider further?**

N/A

2. **Do you have any comments on the individual principles and supporting commentary?**

In general, we support the high-level principles outlined by this consultation as it remains important to have effective governance, risk management and business continuity practices in place to ensure effective operational resilience.

<u>Governance, risk management and planning</u>
The principles encouraging the use of existing governance structures to oversee and implement an effective operational resilience approach is certainly a sound concept. Moreover, we agree that it is important to drive board engagement on this subject and to ensure they can provide effective oversight over the operational resilience strategy. However, whilst we agree that financial institutions should be able to utilise existing practices and structures and drive coordination with business continuity planning, third-party dependency management, recovery and resolution planning and other relevant risk management frameworks, the Committee could have gone further in encouraging a more substantial mindset shift.

The definition supplied by the Committee on operational resilience, and the reference in principle three to business continuity plans, align with traditional business continuity practices rather than assuming the inevitability of disruption and ensuring financial institutions prepare accordingly. We would argue that to ensure effective operational resilience, financial institutions should move beyond siloed approaches to managing risk and maintaining continuity through disruption by ensuring there is a mindset shift filtering down from senior management resulting in an enterprise-wide operational resilience strategy.

<u>Dependencies</u>
A key component of a firm's resiliency is the understanding of their own processes and how they deliver their critical operations. Many firms have recently, or are, in the process of mapping these out and it is therefore welcome that there is consistency with UK regulators in the language used to describe the key areas, 'people, technology, processes, information, facilities'. Similarly, it is right to highlight the reliance on third parties, whether they are outsourced to external suppliers or entities within the same group company.

It is the responsibility of each firm to manage the risk governance of its third-party providers. The widely accepted principle of risk-based proportionality should continue to take account of the relative relationships different firms have with their third-party providers. It is noted that the FCA has granted a three-year transitional arrangement for firms to meet their impact tolerances, acknowledging that large-scale changes, such as moving from one material third party supplier to another, can take time. In that respect, it should also be noted that 'bringing the service back in-house' is not always a viable option.

Incident management and cyber security
It is noted that a bank is required to set a 'risk tolerance for disruption', which differs from the UK's focus on impact tolerances for important business services. As noted earlier, it is assumed that this is driven from a differing regulatory objective on keeping the critical operations functioning from the bank's, rather than the consumer's perspective. It is helpful that there is agreement on duration-based metrics and performance measurements, measuring the expected time to return to business-as-usual.

The content of the incident plan and focus on cyber security as it relates to broader resiliency concerns is also welcomed as it shows the increasing importance of prioritisation on cyber security. This area has historically been frequently overlooked but its significance is vitally important in the resiliency of a firm's critical operations, particularly so in this technological age. Alongside this, it is right to highlight remote working and the associated different considerations that firms have been concerned with in responding to the pandemic.

3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for operational resilience should reflect?

N/A

4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

We would see merit in ensuring an internationally cohesive approach to ensuring effective operational resilience amongst financial institutions. As such, in our broader response we have taken this opportunity to identify important differences between the Committee's and UK regulators' approach to this subject.

5. What kind of metrics does your organisation find useful for measuring operational resilience? What data are used to produce these metrics?

N/A