Daniel Norris and Claire Ward
Prudential Regulation Authority
20 Moorgate
London EC2R 6DA

Governance & Professionalism Policy
Strategy & Competition
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Operational Resilience
Financial Market Infrastructure Directorate
Bank of England
20 Moorgate
London EC2R 6DA

Via Electronic Mail

October 1, 2020

Re: Building Operational Resilience: Impact Tolerances for Important Business Services - Response to UK Consultation Papers

Dear Sirs/Madams,

The Institute of International Finance (IIF) and Global Financial Markets Association (GFMA) ("Industry") appreciate the opportunity to comment on the December 2019 proposals from the Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA) and Bank of England (BoE) – collectively referred to in this letter as the "UK Financial Sector Authorities" – related to strengthening the operational resilience of the UK financial sector.[1]

Operational resilience is a priority for both the private and public sectors to maintain confidence in the financial sector and support financial stability and economic growth through serving the needs of clients. The Industry acknowledges the importance of operational resilience for individual institutions and across the sector as a whole in order to limit harm to firms, customers, markets, the sector, and the broader economies they support nationally and across the globe. Further, as the ongoing COVID-19 crisis has highlighted, the private and public sectors must evolve from viewing risks and threats as being mostly business-specific or geography-specific to thinking about risk and infrastructure on a genuinely global and systemic basis.

The ongoing pandemic further emphasizes the importance of operational resilience. The scale and impact of the pandemic, across different geographies and sectors, demonstrates that firms everywhere need to plan for hazards that can cause significant disruptions. Despite these ongoing extraordinary circumstances, financial institutions have so far remained resilient and adapted with agility, which is a result of significant efforts and investments in the preceding years to build resilient processes, plans,

[1] PRA CP29/19, FCA CP19/32, BoE consultation papers on Operational Resilience: Central Counterparties, Central Securities Depositories and Recognized Payment System Operators and Specified Service Providers.

and communication channels to respond to different types of operational threats and challenges: for example, to enable work from home at scale from the start of the pandemic. Financial institutions have continued to serve clients and the economy despite significant departures from traditional personnel working conditions, increased demands on technology systems, and unforeseen disruptions to supply chains as countries instituted lockdowns. The financial sector has also demonstrated a high degree of cyber resilience despite an upsurge in cyber threats targeting workers in their work from home environments.[2] While firms are continuing to assess the lessons learned from the ongoing pandemic, our members consider that the COVID-19 crisis has underscored the importance of further global consistency and coordination in the policies designed to enhance operational resilience effectiveness and on the intrinsic need for a cross-sectoral alignment on outcomes sought.

Operational resilience is an outcome, not a specific process, and as such the path to maintaining it will differ between firms. Further, operational resilience – like market practices – evolves and matures over time. Given the dynamic nature of operational resilience, the Industry encourages public-private collaboration globally on an ongoing basis. An effective feedback structure that supports continuous dialogue between authorities, policymakers and supervisory teams, and the financial industry is paramount as markets evolve to enable learning from each other and to continually strengthen operational resilience over time. We look forward to continuing to work with the UK Financial Sector Authorities, and other public sector authorities globally, as we collectively work towards maintaining operational resilience outcomes.

IIF and GFMA members are submitting this single response[3] to the UK Financial Sector Authorities' multiple consultation papers relating to the operational resilience of banks, insurers and financial market infrastructure firms.[4]

Our response is organized around six themes:

1. Advantages of a Principles-based, Risk-based and Outcomes-Focused Approach.
2. Mitigating Fragmentation Risk: Promoting Consistent Outcomes Across Jurisdictions, Within Jurisdictions, and with Existing Regulations.
3. Mapping of Assets and Resources to Resilience Outcomes.
4. The Concept of Impact Tolerances: Definition of Harm for Clients, the Market and Individual Firms.
5. Scenario Testing.
6. Governance and Self-assessment.

[2] Industry has shown strong resilience to the recent global DDoS ransom attacks targeting the financial industry and dependent critical infrastructure in other sectors globally, and was also resilient to the global WannaCry and NotPetya ransomware attacks that occurred over three years ago.

[3] This response builds on the global Industry responses to the UK Financial Sector Authorities' 2018 Discussion Paper on *Building the UK financial sector's operational resilience* and also reflects Industry views that were provided in an initial set of *Discussion Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services* published by the IIF and GFMA in October 2019.

[4] PRA CP29/19, FCA CP19/32, BoE consultation papers on Operational Resilience: Central Counterparties/Central Securities Depositories and Recognized Payment System Operators and Specified Service Providers.

The Industry appreciates the UK's thought leadership on how to strengthen operational resilience and their collaborative efforts with both the public and private sectors since the release of the UK Financial Sector Authorities' Discussion Paper in July 2018.[5] As other jurisdictions and global standard setters publish their views on strengthening operational resilience, we encourage the UK to continue to actively engage with the members of the global working groups in which the UK participates, for example through the Basel Committee on Banking Supervision (BCBS),[6] in pursuit of as much regulatory alignment as possible on the outcomes sought and how to demonstrate resilience across jurisdictions.

We would like to emphasize the following key messages:

- The need for regulatory consistency, internationally and within jurisdictions, given that a financial firm's businesses and associated processes may span multiple geographies.
- The importance of continued public-private collaboration on the UK's new operational resilience concepts, including beyond the consultation period: this will be an iterative process and it will take time to mature what are some new and complex concepts.
- Operational resilience should focus on the alignment of outcomes that promote financial and market stability as well as firm safety and soundness by protecting and resuming key services during operational disruptions, enabling firms to continue serving the needs of their clients.
- The desire to continue striving for a principles-based, risk-based and outcomes-focused approach where firms have the flexibility to determine the specifics of their own operational resilience programs in a way that is relevant and proportionate to their business and risk profile, including leveraging existing broader risk management frameworks acknowledging that these may need to be augmented or supplemented with a new but compatible framework, as necessary.
- The Industry needs flexibility on how firms demonstrate resilience outcomes (i.e., principles-based, without prescribing specific metrics), allowing the necessary time for collaboration with supervisory teams (potentially cross-border) and a thoughtful implementation timetable.

1. Advantages of a Principles-based, Risk-based and Outcomes-Focused Approach

At its core, operational resilience should focus on outcomes that promote financial and market stability as well as firm safety and soundness by protecting and resuming key services during operational disruptions, enabling firms to continue serving the needs of their clients. Agreeing on a consistent outcome sought, or aligned approaches to demonstrate operational resilience, across firms and across jurisdictions would:

- Provide a minimum agreed upon outcome objective for the definition and measurement of operational resilience, which would foster market confidence and global financial stability;
- Increase comparability across jurisdictions, enabling understanding and accurate communication;
- Minimize the impacts of cross-border disruptions and global firmwide disruptions; and

[5] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.
[6] In August 2020, the BCBS release a consultative document: "Principles for Operational Resilience".

- Result in better resilience outcomes, reduce risks, and create efficiencies for the Industry and regulatory community alike.

Globally, financial sector firms have different business models and organizational structures and therefore a principles-based, risk-based and outcomes-focused framework is necessary to best support global consistency. As expressed in the UK Financial Sector Authorities' consultation papers, firms would like the flexibility to determine the specifics of their own operational resilience programs in a way that is relevant and proportionate to their unique business and risk profile. Specifically, it is necessary to give firms flexibility to align, where applicable and not as a requirement, with existing processes that they have built to comply with existing standards, regulations and guidance, such as for Business Continuity Planning (BCP) and Recovery and Resolution Planning (RRP). Some firms intend to leverage and align to existing internal structures when strengthening operational resilience and would like express supervisory permission to do so.

The Industry would like regulatory policy and supervisory teams' mandates to include supporting the flexibility of firms to evaluate the resilience of key services as markets evolve. Acknowledgment of the value of such flexibility incentivizes the financial industry to continuously adapt, in collaboration with other market participants and regulatory authorities, and to maintain a high level of resilience in the highly dynamic environment in which they operate.

The Industry believes that the development and documentation of operational resilience programs should not become overly burdensome and should respect the sensitive and confidential nature of the data contained in the documentation. To the extent that firms can use the same submissions to supervisors in different jurisdictions, this would significantly reduce burden. This should be feasible if authorities align on a principles-based, risk-based and outcomes-focused framework that is globally consistent.

2. Mitigating Fragmentation Risk: Promoting Alignment of Outcomes Across Jurisdictions, Within Jurisdictions, and with Existing Regulations

The potential for fragmentation due to divergences in regulatory standards and supervisory oversight poses substantial risks and operational challenges for financial services firms that operate globally and, in turn, for the strength of the financial system. Alongside the UK Financial Sector Authorities' proposals, other related approaches are being advanced by authorities in various jurisdictions, including the European Union,[7] Singapore,[8] and Canada[9].

Specifically, the Industry is conscious that if national level approaches are developed in isolation, without aligning to a globally agreed outcome sought, the resulting fragmentation could undermine the strength of the financial sector's operational resilience efforts, including during cross-border disruptive events. More generally, fragmentation resulting from excessive regulatory and supervisory divergence can create significant financial, operational, and risk

[7] EU draft regulation on digital operational resilience for the EU financial services sector (DORA), September 24th, 2020.
[8] Monetary Authority of Singapore: Ensuring Safe Management and Operational Resilience of the Financial Sector (April 2020).
[9] Canadian OSFI consultation on technology risks in the financial sector, September 15th, 2020: https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/med/Pages/tchrsk-nr.aspx.

management inefficiencies resulting in additional unnecessary costs and reduced capacity for financial firms to serve domestic and international customers.

The Industry would like greater clarity on the degree of alignment of outcomes sought between the various operational resilience policy initiatives that are in flight. The BCBS has released a consultation on global principles for operational resilience; we encourage the UK Financial Sector Authorities to continue to engage through the BCBS working group to support globally aligned objectives. This alignment is important and necessary to mitigate the extraterritorial impacts of jurisdiction-specific approaches.

The Industry sees operational resilience as a rare opportunity for regulatory and supervisory coordination and collaboration from the start to increase comparability across jurisdictions. We would like to propose some practical suggestions to the UK Financial Sector Authorities, and other authorities globally, to keep up the momentum for the mutual benefit of reinforcing market confidence.

- ***Increase public/private sector collaborative engagement, with a cross-border dimension***

The Industry believes it will be essential to partner with the public sector authorities to support global coordination efforts and strengthen operational resilience. Joint industry and regulatory collaboration across jurisdictions is critical to negate the risk of unnecessary complexity, regulatory divergence, increased cost and effort that ultimately affects progress and could hamper efforts to manage cross-jurisdictional disruptions. In the UK, the Cross Market Operational Resilience Group (CMORG) is an excellent example of the ongoing detailed level of public/private engagement this important matter needs to mature operational resilience concepts. We would encourage similar collaborations on an international level, including specific analysis of cross-border issues.

There is precedent for fruitful cross-country collaborative projects between the public and private sectors in related fields. The financial sector has worked closely with regulatory authorities around the world to ensure supervisors meet their regulatory objectives and that proposed rules, regulations or guidance are practical, efficient, effective, implementable and do not cause unintended consequences. For example, U.S. regulators are now piloting Coordinated Cyber Reviews to reduce the number of duplicative cyber exams occurring within the same G-SIB. Along with this, U.S. Regulators have also agreed to accept as evidence the industry-developed Financial Sector Profile, a set of over 250 financial-sector specific cyber controls intended to improve uniformity and overall cyber resiliency. Using a financial firm's self-assessment against the Profile eliminates the need for examiners to repeatedly ask basic security questions, providing significant efficiencies for both regulators and financial firms.[10] There are many other examples we could share given the financial sector's long history of actively collaborating with regulatory authorities where firms and regulators have a shared interest in keeping the financial sector secure and operational, especially during periods of disruption.

[10] Previous studies have shown that, in some member firms, nearly 40% of a financial firm's cyber staff today are responding to regulatory requests rather than being on the front lines building stronger cyber defenses.

- ***Avoid creating fragmentation or conflicts with existing standards, regulations, guidance***

Firms are already subject to a wide range of regimes that are integral processes to the current and future strength of operational resilience. These include, but are not limited to, operational risk, risk appetite, enterprise risk management (ERM), BCP, cyber and information and communication technology (ICT) security, IT resilience, disaster recovery, third-party vendor management and RRP. See the Appendix for an indicative, non-exhaustive list of relevant regulations and guidance that financial firms already comply with globally and that reflect the resilience capabilities firms have already developed over time. These existing regimes are themselves somewhat different and fragmented across jurisdictions; to introduce further fragmentation through lack of consistent alignment on new operational resilience outcomes sought would only compound existing challenges for global firms and undermine the objective to strengthen operational resilience.

- ***Avoid fragmentation through use of similar terminology***

Clear use of terminology is an important part of avoiding fragmentation. The Industry particularly urges the UK Financial Sector Authorities, and global authorities more generally, to consider how any new terminology created as part of operational resilience policy development translates to terms that are used in existing regulatory standards, requirements and guidelines, to the extent that they already exist. We also urge authorities to avoid using different terms in different jurisdictions to refer to the same concepts.

More generally, the Industry would call on the UK Financial Sector Authorities (and supervisors in other jurisdictions) to look through any differences in terms that may exist and focus on assessing whether firms can demonstrate that the desired resilience outcomes are being achieved.

- ***Seek alignment between policy and supervision teams within jurisdictions***

As well as international alignment, the Industry would like to reduce fragmentation within individual jurisdictions and would also advocate for alignment of approaches between policy and supervision teams. In the case of the UK, the Industry would encourage closer and clearer alignment between the proposed policy and supervisory approaches of the PRA and FCA. To avoid operational resilience developments becoming a compliance-driven exercise it is crucial that supervisory teams acknowledge the iterative nature of the implementation and, therefore, reflect this flexibility when supervising individual firms.

- ***Reflect the dynamic nature of the policy development, including with a thoughtful approach to implementation***

The Industry views operational resilience maturity as an iterative process that will continue to evolve. Regulatory and supervisory expectations should allow for and encourage firms to consistently review and enhance their programs rather than focus on a static point in time for demonstrating operational resilience. Prioritizing efforts to achieve and demonstrate operational resilience should be done in collaboration with authorities on a cross-border basis to identify any current gaps, where the timeline for the closure of such gaps should be based on the potential severity to both the firm and the sector rather than by a fixed date for all gaps and all firms. To address certain gaps, some firms may need to make significant investments and major technological or organizational changes. Such changes would inevitably require a thoughtful implementation period to execute in

parallel to maintaining ongoing resilience management, particularly for large firms and those operating cross-border.

In the UK context, it would be helpful for the UK Financial Sector Authorities to take a phased approach to implementing the UK operational resilience approach and in firm supervision. Setting clear outcomes-focused expectations and milestones in relation to these phases, rather than the current emphasis in the consultation papers on overall compliance within a maximum of three years of when the final rule comes into force, will facilitate firms dedicating time, effort and investment on a cost-efficient and proportionate basis as they enhance their operational resilience programs. In particular, the final rule should allow for the necessary flexibility in timelines so firms can implement the appropriate controls and responses that will benefit the firm's resilience over the long-term, rather than implementing short-term measures simply to meet compliance requirements and estimated timelines.

The following comments under Themes 3 to 6 reflect the points of broad agreement between IIF and GFMA members on each. The comments are not all-inclusive of all open issues and therefore do not reflect the full breadth of Industry views on these complex topics, recognizing that this is an iterative process and, in time, the Industry seeks greater alignment and ongoing collaboration with authorities. We hope the comments provided are valuable in highlighting points of commonality of views by the Industry at this time.

3. Mapping of Assets and Resources to Resilience Outcomes

Important Business Service Concept

The Industry believes that important business services, or the like, should be determined by each firm based on the services it delivers to customers, and proportionately to the firm's business and risk profile and its role in the broader market. We agree with the sentiment in the UK consultations that – depending upon their role in the financial system – some firms may not have as many, or the same, important business services as others.[11] Some firms may choose to leverage their existing RRP or ERM governance structures to help identify an important business service, or the like.

In general, the Industry thinks that it would be preferable to focus important business services, or the like, on the outcomes clients and markets require that firms fulfil by providing financial services – e.g. access to cash, ability to pay bills, etc. Prioritizing resources on an outcomes-focused approach to defining important business services, or the like, would also help maintain a manageable scope of a firm's operational resilience processes and direct resource and investment to those integral to the safety and soundness of firms and financial stability in serving client's needs.

The Industry thinks that it will take some time to clarify, through further discussion between firms and supervisors, the concept of important business services, or the like, and demonstrate that they are captured in achieving operational resilience outcomes.

[11] For example, see PRA CP29/19 states that *"(t)he PRA does not propose to introduce definitive lists or taxonomies of important business services, as specifying certain services as important in all circumstances is unlikely to be proportionate. For example, because firms have differing business models, the same business service may be important for one firm but not another."*

Mapping

Mapping is an important process that supports assessment of the resources that are critical to delivering a service to clients; firms already rely on mapping as part of their BCM and for the RRP framework. There is value in a proportionate approach to mapping certain dependencies as there are inherent differences in the complexity between, for example, the mapping of data and information compared to other dependencies (such as facilities and legal entities). In addition, mappings contain highly sensitive information, therefore appropriate safeguards need to be in place to protect them. It will be important for the UK Financial Sector Authorities to collaborate with firms to clarify the mapping requirements necessary to demonstrate resilience has been achieved.

The Industry emphasizes the value in firms developing their own approaches to mapping, as no singular approach to mapping will apply across the Industry. As the UK Financial Sector Authorities recognize in their consultation papers,[12] mappings are firm-specific: the purpose is to look at the services firms provide to their clients and ensure they can identify exactly how they are delivered during business as usual, and how they would be delivered under disrupted conditions. Some firms already map upstream and downstream internal business process and external ecosystem dependencies, and qualitative and quantitative impacts (e.g. financial consequence of loss over time), when they develop their business continuity plans as part of what is called the business impact analysis and risk assessment. These analyses can help inform business continuity plans as well as identify potential vulnerabilities for disruption. While a baseline for mapping for comparability purposes is valuable, there are many different ways to undertake a mapping exercise since mappings are firm-specific and will, therefore, differ across the financial sector.

Third Party Providers

We applaud the UK Financial Sector Authorities for approaching the operational resilience of the entire system in its consultation policy proposals – including banks, insurers and financial market infrastructures (FMIs). The UK Financial Sector Authorities state that mapping should allow firms to identify vulnerabilities from, among other things, concentration risks and dependencies on third parties.[13] However, firms often are not able to contractually request or require all the necessary information from their third or fourth parties and have a limited ability to assess aggregate risk.

It would therefore be helpful for the UK Financial Sector Authorities – in collaboration with other authorities globally – to convene with financial institutions and important third parties to support information sharing and the assessment of sector-wide risks, including potential risks that would be outside an individual firm's purview. The ability for regulators and supervisors to foster this transparency would be particularly valuable to enhance authorities' assessment of financial stability risks, and to assist firms in the development of appropriate metrics accounting for relevant externalities.

---

[12] For example, PRA CP29/19 paragraph 5.6 states that *"Firms should document their mapping in a way that is proportionate to their size, scale and complexity. Firms are expected to develop their own methodology and assumptions for mapping to best fit their business."*

[13] The PRA is consulting separately on Outsourcing and Third Party Risk Management in CP30/19, which was published alongside the UK consultations on Operational Resilience. The Association for Financial Markets in Europe (AFME), as a member of the GFMA alliance, encourages the PRA to read AFME's response to CP30/19 where specific comments and recommendations have been made regarding third party arrangements.

4. The Concept of Impact Tolerances: Definition of Harm for Clients, the Market and Individual Firms

In the consultation papers, the UK Financial Sector Authorities are proposing Impact Tolerances as a new concept to articulate and demonstrate operational resilience.

Firms will require flexibility to integrate this concept into their own business and existing processes, including the ability to leverage their broader risk management frameworks, acknowledging that these may need to be augmented or supplemented with a new but compatible framework, as necessary. Firms should define their own tolerances, or the like, using appropriate metrics. When looking across firms, it will be important to account for the different roles that firms play in the market in the provision of services.

The Industry thinks it is crucial to maintain flexibility for individual firms to use and evolve metrics[14] over time as part of their operational resilience programs. The Industry does not think that mandating certain metrics for regulatory or supervisory purposes will further the ultimate objectives of operational resilience. The Industry believes that regulators and supervisors should review evidence as to how firms are managing their own risk and not be prescriptive on metric design and definitions. Defining metrics would not allow for the nuances across firms to be addressed, makes it more complex to make any in-flight changes during an incident, and any necessary changes to the metrics could be slow and bureaucratic. Providing firms with the necessary flexibility to account for the way different scenarios affect their important business services, clients, business and broader markets and financial stability is important rather than having an excessive focus on technical resumption decisions driven by certain metrics.

In their consultative document, the BCBS state that *"further work is required to develop a reliable set of metrics that both banks and supervisors can use to assess whether resilience expectations are being met"* and does not therefore propose any metrics at this time. The Industry agrees that more work is needed to assess the appropriate role for, and choice of, various metrics to allow firms and supervisors to reliably assess whether operational resilience expectations are being met.

Concept of consumer harm, as proposed by the FCA

Minimizing disruptions for clients – retail or wholesale – is clearly front and center in firms' minds when considering the operational resilience of their business services. However, the Industry thinks there are open questions about whether and how to account for 'consumer harm' when defining important business services and setting impact tolerances. Specifically, a 'tolerable' or 'intolerable' level of harm (to use the FCA's terms; the PRA, on the other hand, refers to 'maximum acceptable level of disruption') is not currently widely understood in the global financial industry. Further, firms believe there is a difference between consumer inconvenience and harm depending on the nature and duration of an outage: firms seek to avoid either outcome as a result of operational incidents, but consumer harm is clearly more serious. The industry would like clarity on the point at which the FCA considers harm to occur. Firms continue to focus on having several options available to provide the outcomes clients require (access to cash, ability to make payments, etc.), which can also lessen the impact on clients during a disruption. Additionally, the concept of harm may be more challenging in relation to firms' wholesale activities, where the definition of consumer harm is even more difficult to specify than it is in retail banking.

[14] PRA CP29/19: *"(3.10) Firms should state their impact tolerances using clear metrics. … (3.11) The PRA expects firms to use a time-based metric for all impact tolerances, but in some cases, firms may find it suitable to use this in combination with other metrics."*

With respect to the UK Financial Sector Authorities' proposals to potentially require up to two impact tolerances per important business service, the Industry thinks that this regulatory approach would unnecessarily complicate implementation in the UK. The Industry also thinks that dual-regulated firms may come to the view that, after testing, the second (more severe) impact tolerance is not necessary. Besides the implementation issues, having a distinct approach to dual-regulated UK groups would also make the UK's framework bespoke to its own institutional set-up, which would affect UK firms with global operations and will drive a wedge with other jurisdictions.

5. Scenario Testing

The Industry agrees on the importance of scenario testing. A primary objective of testing is for firms to understand whether their important business services, or the like, can withstand severe but plausible disruptions, and what vulnerabilities or dependencies need to be addressed to further support operational resilience in the event of a real disruption.

Firms already routinely perform a variety of internal testing of their resilience and contingency plans as part of their BCP and other programs. The range of scenarios that firms could consider when assessing and building their operational resilience capabilities is extremely large. Firms should, in collaboration with supervisors, identify scenarios and types of disruptions that are the most relevant to their business and risk profile and continue to prioritize resources and investment to strengthen their operational resilience maturity where it is most warranted based on the importance of services to the firm, clients and the sector. It may be more tractable for firms to avoid developing specific scenarios and rather to focus on a range of possible disruptions e.g. loss of a certain amount and type of data, technology and personnel.

In general, testing should be done on the basis of a "do no harm" principle. For example, testing live systems in a production environment can itself potentially increase the risk of disruption to a firm's ability to deliver services**. Testing requirements should also be proportionate: for many purposes, table-top exercises and simulations would be sufficient, particularly in the context of cross-sectoral testing, while other components of the scenario may require more sophisticated testing.** The ability to fully test and evidence outcomes without injecting failure into the organization requires significant development.[15]

In addition, the interpretation of what is considered "plausible" in relation to severe but plausible scenarios will be firm specific. The UK consultations refer to a firm increasing the severity of a testing scenario by assuming simultaneous disruptions to key firm resources, or extending the period for which a particular resource is unavailable.[16] We think it should be up to firms to determine the degree of severity that would still be plausible.

Testing could be conducted both at the level of individual firms as well as at the level of the financial sector to support preparedness and identify interconnections and potential market dependencies. The Industry believes scenarios should reflect the fact that incidents do not stop at borders and that there are interdependencies between financial sector participants and other important sectors. Eventually scenario testing could be conducted with financial institutions' non-bank third

[15] Whilst internally some firms may already be testing to different levels and have technical solutions for failure injection across some technology, this will not be consistent. Non-technology testing is usually manual and done to minimize impact on the day-to-day business.
[16] PRA CP29/19, paragraph 4.21.

party providers including critical utilities, critical infrastructure and critical shared services to allow for system-wide testing and monitoring. This is another important reason for ongoing global collaboration and the necessity for alignment of outcomes sought.[17]

6. Governance and Self-assessment

The Industry agrees with the UK consultation papers that a firm's board should be informed about the objectives of operational resilience and the firms' specific efforts in order to approve strategic prioritization on investment decisions and to provide a credible challenge to the business functions that develop the detailed operational resilience processes and perform mapping and testing.

While there needs to be board-level and senior leadership awareness and support for operational resilience, it is important to ensure alignment with existing governance structures. Firms are leveraging internal governance structures (and requirements such as the Senior Managers Regime in the UK) to provide various stakeholders – including boards, executive leadership and regulatory authorities – with visibility into evolving resilience risks to facilitate timely management. Firms are integrating resilience into the culture of their core business operations and risk management.

The Industry strongly believes that operational resilience management should not be a check-the-box compliance exercise and firms will need to monitor and manage their operational resilience programs on an ongoing basis.

(Continued overleaf)

[17] In their consultative document, the BCBS states that they aim to *"strengthen operational resilience by furthering international engagement and seeks to promote greater cross-sectoral collaboration over this body of work."* (Paragraph 4.)

Concluding remarks

The IIF and GFMA reiterate our members' support for advancing operational resilience in the global financial sector, and we hope our comments are helpful in enhancing the debate on operational resilience. It is widely recognized that strengthening operational resilience will be an iterative process that requires effective collaboration among financial institutions and regulators around the world on an ongoing basis. This process is already underway through valuable efforts such as the CMORG in the UK. As and when other jurisdictions create similar public-private sector working groups, we hope their mandates will also include a cross-border component. The focus must always be on delivering tangible, outcomes-focused results that achieve genuine resilience enhancements. Continuing this collaborative engagement with a focus on the outcomes for clients, markets and financial stability gives the highest chance of success.

As always, we are available to provide any necessary expansions and/or clarification on our comments, and we welcome future continued dialogue on how supervisors and market participants may move forward most effectively to further support operational resilience across the financial sector.

Sincerely,

Allison Parent
Executive Director
Global Financial Markets Association (GFMA)
aparent@gfma.org

Martin Boer
Director, Regulatory Affairs
Institute of International Finance (IIF)
mboer@iif.com

APPENDIX

This appendix does not include the UK Financial Sector Authorities' proposals, which are the subject of the main letter, but includes other relevant documents for context.

Financial Regulations and Resilience Capabilities by theme/functional area		
Functional Area	**Regulation/Guidance**	**Resilience Capabilities**
Operational resilience	Basel Committee on Banking Supervision (BCBS) – Principles for Operational Resilience (August 2020)	• Seeks to promote a principles-based approach to improving operational resilience. • Build on the Committee's Principles for the Sound Management of Operational Risk (PSMOR), principles on corporate governance for banks, outsourcing, business continuity and relevant risk management-related guidance.
	Monetary Authority of Singapore (MAS) - Ensuring Safe Management and Operational Resilience of the Financial Sector (2020)	• Issue guidance and advisories to address operational, technology and cyber risks. • Focus our surveillance, supervision and enforcement efforts on financial institutions' pandemic response as well as operational and cyber resilience. • Continue to monitor the impact of COVID-19, and put in place additional measures and advisories as necessary.
	European Commission – Digital Operational resilience framework for financial services (December 2019)	• Propose targeted improvements of ICT and security risk management requirements. • Harmonize reporting of ICT incidents. • Develop a harmonized digital operational resilience testing framework. • Enhance oversight of critical third-party providers.
Risk Governance	Basel Committee on Banking Supervision (BCBS) – Corporate Governance Principles for banks (July 2015)	• Ensure sound and robust corporate governance by determining allocation of authority and responsibilities, including: i/ setting the banks strategy and objectives; ii/ selecting and overseeing personnel; iii/ operating the bank on a day-to-day; iv/ protecting recognized stakeholders; v/ aligning corporate culture; vi/ establishing control functions. • Reinforce the collective oversight and risk governance responsibilities of the board (e.g. risk governance, risk culture, risk appetite, risk capacity). • Evaluating and promoting a strong risk culture in organizations.
	Financial Conduct Authority (FCA) - The Senior Managers and Certification Regime (July 2019)	• Provide a robust framework for accountability and transparency • Ensure accountability from the most senior individual responsible for managing the internal operations and technology of a firm.
	Federal Reserve Board (FRB) – 'Three Lines of Defense' Risk Management Model	• Ensure systemically important financial institutions (SIFIs) manage risk in a way that is prudent and consistent with their business strategy and risk tolerance. • Clarify the responsibility of the executive management team in managing the overall risk framework.
	The Office of the Comptroller of the Currency (OCC) - Heightened Standards for Large Financial	• Guidelines to strengthen the governance and risk management practices of large financial institutions. • The guidelines provide that covered institutions should establish and adhere to a written risk governance framework to manage and control its risk-taking activities.

	Institutions (September 2014)	• The guidelines also provide minimum standards for the institutions' boards of directors to oversee the risk governance framework.
	IAIS – Application Paper on Proactive Supervision of Corporate Governance (February 2019)	• calls upon insurance supervisors to be forward-looking, identify issues early and to act quickly and constructively to address circumstances before they become critical or a violation of law or local requirements.
Risk Monitoring and Management	FSB – Principles for an effective risk appetite framework (November 2013)	• The FSB Principles set out key elements for: (i) an effective risk appetite framework, (ii) an effective risk appetite statement, (iii) risk limits, and (iv) defining the roles and responsibilities of the board of directors and senior management. • The Principles aim to enhance the supervision of systemically important financial institutions but are also relevant for the supervision of financial institutions and groups more generally, including insurers, securities firms and other non-bank financial institutions.
	Basel Committee on Banking Supervision (BCBS) - Principles for the Sound Management of Operational Risk (June 2011)	• Ensure that financial institutions identify risks to the bank and measure exposures to those risks (where possible), and ensures that an effective capital planning and monitoring program is in place to monitor risk exposures and corresponding capital needs on an ongoing basis, take steps to control or mitigate risk exposures and report to senior management and the board on the bank's risk exposures and capital positions.
	Basel Committee on Banking Supervision (BCBS) - Revisions to the principles for the sound management of operational risk (August 2020)	• Review principles that have not been adequately implemented, and issue further guidance to facilitate implementation (e.g. risk identification and assessment tools, change management programs and processes, implementation of the three lines of defense, senior management oversight, articulation of operational risk appetite and tolerance statements, risk disclosure). • Capture additional important sources of operational risk, such as those arising from information and communication technology (ICT) risk, warranting the introduction of a specific principle on ICT risk management.
Busines Continuity Planning, Systems Integrity and Third-Party Resilience	The Joint Forum (BCBS, IOSCO, IAIS) – High-Level Principles for Business Continuity (August 2006)	• Ensure the development of recovery objectives that reflect the risk an event represents to the economy. • Require the conducting of periodic tests of business continuity plans to ensure the plans are effective.
	The Joint Forum (BCBS, IOSCO, IAIS) – Outsourcing in Financial Services (February 2005)	• Reduce potential for over-reliance on outsourced activities that are critical to the ongoing viability of a regulated entity (e.g. draw up comprehensive and clear outsourcing policies, establish effective risk management programs, require contingency planning by the outsourcing firm, negotiate appropriate outsourcing contracts, and analyze the financial and infrastructure resources of the service provide). • Mitigate concerns by ensuring that outsourcing is adequately considered in firm assessment whilst taking account of concentration risks in third party providers when considering systemic risk issues.
	IOSCO – Principles on Outsourcing:	• Set out expectations for regulated entities that outsource tasks, along with guidance for implementation. • Seven fundamental principles covering issues such as the definition of outsourcing, assessment of materiality and criticality, affiliates, sub-contracting and outsourcing on a cross-border basis.

	Consultation Report (May 2020)[18]	
	Federal Financial Institutions Examination Council (FFIEC) – Business Continuity Guidelines	• Decrease the likelihood that disruptions will have a material and long-lasting impact on critical business services. • Require institutions to assess all business functions, identify the impact of business disruptions and estimate maximum allowable downtime and recovery time objectives.
	Federal Financial Institutions Examination Council (FFIEC) - Information Technology Examination Handbook: Business Continuity Management	• Describe principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. • Focus on enterprise-wide, process-oriented approaches that consider technology, business operations, testing, and communication strategies critical to the continuity of the entire entity.
	Federal Reserve System, U.S. Treasury Office of the Comptroller of the Currency, and the Securities and exchange Commission (SEC) – Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (April 2003)	• Ensure rapid recovery and timely resumption of critical operations and staff following a wide-scale disruption for firms that play significant roles in critical financial markets. • Require firms a high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.
	Monetary Authority of Singapore (MAS) - Business Continuity Guidelines (June 2003)	• Ensure BCM is a risk-based framework that addresses operational risk by developing clear policies, strategies, and accountabilities for the recovery of critical business functions.
	Monetary Authority of Singapore (MAS) – Proposed revisions to guidelines on Business Continuity Management (March 2019)	• Set expectations of how an FI's are to identify business functions that are critical and prioritize for recovery in disruption. • Place greater emphasis on the Board of directors and senior management to demonstrate leadership and commitment in building an organizational culture that embeds business continuity. • Expect FIs to have in place end-to-end business continuity plans for each service that is delivered to their customers. • Continue to expect an FI to conduct different types of testing to gain the confidence that they will be able to continue to operate reliably, responsively, and efficiently as planned.
	Security Exchange Commission (SEC) – Regulation Systems Compliance and Integrity (Regulation SCI) (February 2015)	• Requires SCI entities (including registered clearing agencies) to establish written policies and procedures reasonably designed to ensure their systems have levels of capacity, integrity, resilience, availability and security adequate to maintain their operational capability. • Require SCI entities to mandate participation by designated members or participants in scheduled testing of the operation of their BC/DR plans, including backup systems, and to coordinate such testing on an industry- or sector-wide basis with other SCI entities.

[18] GFMA responded to the IOSCO consultation report on Principles for Outsourcing on September 30th, 2020. Please find the response here: https://www.gfma.org/wp-content/uploads/2020/09/gfma-response-iosco-principles_on_outsourcing_cp.pdf.

		• Require SCI entities to develop business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption.
	European Banking Authority (EBA) - Outsourcing Guidelines (February 2015)	• Set standards for the management of outsourcing risk. • Define requirements for competent authorities to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring risk concentrations at individual service providers and assessing whether or not such concentrations could pose a risk to the stability of the financial system.
	European Securities Market Authority (ESMA) - Draft Guidelines on Outsourcing to Cloud Service Providers (June 2020)	• Develop guidance on outsourcing to cloud service providers. • Support firms identify, address and monitor the risks that may arise from their cloud outsourcing arrangements.
	Prudential Regulatory Authority (PRA) – Outsourcing and third party risk management (December 2019)	• Complement proposals on operational resilience • Facilitate greater resilience and adoption of the cloud and other new technologies. • Implement EBA 'Outsourcing Guidelines' with consideration to, proportionality, governance / record keeping, outsourcing arrangements, data security, access / audit / information rights, sub-outsourcing, business continuity / exit planning.
	EIOPA – Guidelines on Outsourcing Cloud Service Providers (February 2020)	• EIOPA Guidelines provide direction on cloud services and outsourcing, including the need for: a thorough pre-outsourcing analysis and risk assessment; a written outsourcing policy; notification to the supervisory authority of the outsourcing of critical or important operational functions and activities to Cloud Service Providers (CSPs); documentation requirements; due diligence and contractual considerations; exit strategies; access and audit rights; and data and system security.
Cyber Resilience and Risk Management	FSB – Cyber Lexicon (November 2018)	• Set of 50 core terms related to cyber security and cyber resilience. • Support the work of the FSB, standard-setting bodies, authorities and private sector participants, to address financial sector cyber resilience.
	FSB – Effective Practices for Cyber Incident Response and Recovery (April 2020)	• Provide a toolkit of effective practices to assist financial institutions before, during and after a cyber incident. • Set 46 effective practices, structured across: i/ Governance; ii/ Preparation; iii/ Analysis; iv/ Mitigation; v/ Restoration; vi/ Improvement; vii/ Coordination and communication.
	G7 - Fundamental Elements of Cybersecurity for the Financial Sector (October 2016)	• Require firms to identify functions, activities, products and services — including interconnections, dependencies, and third parties — prioritize their relative importance and assess their respective cyber risks. • Require firms to identify and implement controls — including systems, policies, procedures and training — to protect against and manage cyber risks within the tolerance set by the governing authority.
	G7 – Fundamental Elements for effective	• Describe desirable outcomes for mature entities: i/ G7 fundamental elements are in place; ii/ cybersecurity influences organizational

	assessment of Cybersecurity in the Financial Sector (October 2017)	decision-making; iii/ understanding that disruption will occur, iv/ an adaptive cybersecurity approach is adopted; v/ there is a culture that drives secure behaviors. • Provide assessment components for assessors, to develop approach to assessing progress as entities build and enhance their cybersecurity: i/ establish clear assessment objectives; ii/ set and communicate methodology and expectations; iii/ maintain a diverse and process for toolkit selection; iv/ report clear findings and concrete remedial actions; v/ ensure assessments are reliable and fair.
	G7 – Fundamental Elements for threat-led penetration testing (October 2018)	• Provide guidance for the assessment of resilience against malicious cyber incidents through simulation and testing (Threat-Led Penetration Testing). • Enhance and assess cyber resilience of entities in the financial sector through guidance on: i) scoping and risk management; ii) resourcing; iii) threat intelligence; iv) penetration testing; v) close and remediation; vi) thematic data.
	Bank of England (BoE) CBEST (2016) European Central Bank (ECB) TIBER-EU (May 2018)	• Provide standard approaches for regulatory-driven penetration testing regimes.
	European Central Bank (ECB) Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE) (December 2018)	• Set standards for the management of cybersecurity risks. • Provide FMIs with detailed steps on how to operationalize the guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time. • Provide overseers with clear expectations to assess the FMIs for which they are responsible. • Provide the basis for a meaningful discussion between the FMIs and their respective overseers.
	IAIS – Application Paper on Supervision of Insurer Cybersecurity (November 2018)	• Provides 7 elements of insurer cybersecurity practices: a strategy and framework; governance; risk and control assessment; monitoring; response; recovery; information sharing and continuous learning. • The Application Paper also includes supervisory case studies of effective practices. It notes that cyber resilience must be achieved by all insurers, regardless of size, specialty, domicile or geographic reach. Supervision of cyber resilience should be proportionate and risk-based.
Technology Risk Management	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019)	• Sets minimum standards for the management of Information and Communication Technology (ICT) and security risk management. • Sets expectations in relation to governance, the risk assessment process, information security requirements, ICT operational management, security in the change and development processes and business continuity management to mitigate ICT and security risks.
	Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices – Technology Risk (June 2013)	• Guidance on the oversight of technology risk management, security practices and controls to address technology risks.

	IAIS – Application Paper on the Use of Digital Technology in Inclusive Insurance (November 2018)	• Discusses digital technology applications in an inclusive insurance context and how the Insurance Core Principles can be applied in a proportionate manner in the supervision of the use of digital technologies in inclusive insurance. An Annex to the paper discusses the risks manifest in digital technology applications.
FMI Resilience	The International Organization of Securities Commissions (IOSCO) Principles for Financial Market Infrastructures (PFMI) (April 2012)	• Ensure the security of critical functions and, in the event of a disruption, recovery of operational capacity in a timely manner. • Require review of the entity's material risk exposure as a result of interdependencies with other entities. • Require identification of events that prevent an entity from providing its critical operations and services as a going concern.
	Committee on Payments and Market Infrastructures (CPMI) & International Organization of Securities Commissions (IOSCO) - Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016)	• Supplemental details, on top of the Principles for Financial Market Infrastructures (PFMI) [see row above], related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability. • Outlines 5 risk management categories that should be addressed across FMI's cyber resilience framework: governance; identification; protection; detection; and response and recovery. Also outlines 3 overarching components: testing; situational awareness; and learning and evolving.
Stress Testing	BCBS – Stress Testing Principles (October 2018)	• The principles are guidelines that focus on the core elements of stress testing frameworks. These include the objectives, governance, policies, processes, methodology, resources and documentation that guide stress testing activities and facilitate the use, implementation and oversight of stress testing frameworks.
	Bank of England - The Bank of England's approach to stress testing the UK banking system (October 2015)	• Stress tests therefore contribute to the Financial Policy Committtee's statutory objective to protect and enhance the stability of the UK financial system, and, subject to that, support the economic policy of the Government. Equally, they contribute to the PRA's general objective to promote the safety and soundness of the banks it regulates, and its secondary objective to facilitate effective competition in the markets for services by the banks it regulates.
	Federal Review Board (FRB) - Comprehensive Capital Analysis and Review (CCAR)	• Ensures that banks have adequate capital to absorb losses and are able to lend to households and businesses even in a severe recession. • Ensures that the largest and most systemically important financial institutions are able to continue to operate under severe economic stress conditions. • Promotes financial resilience that indirectly supports operational resilience by ensuring necessary resources to support operational capacity.
	Federal Review Board (FRB) - Comprehensive Liquidity Analysis and Review (CLAR)	• Ensures the largest and most systemically important financial institutions' ability to continue to operate under severe liquidity stress. • Requires firms to assess the adequacy of their liquidity positions relative to their unique risks and tests the reliability of these institutions' approaches to managing liquidity risk. • Promotes financial resilience that indirectly supports operational resiliency by ensuring necessary resources to support operational capacity.
Recovery and Resolution	FSB - Guidance on Arrangements to Support	• Identify a number of arrangements including specific contractual provisions, access arrangements and governance structures that, if

	Operational Continuity in Resolution (August 2016)	implemented appropriately, could support operational continuity in resolution.
	FSB - Key Attributes of Effective Resolution Regimes for Financial Institutions (October 2014)	• Set out core elements considered to be necessary for an effective resolution regime.
	FSB - Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services (July 2013)	• Provide basis for a strategic analysis that identifies firm's essential and systemically important (or "critical") functions. • Assist evaluation of firm's criticality of functions. • Promote common understanding of which functions and shared services are critical by providing shared definitions and evaluation criteria.
	European Commission - Bank Recovery and Resolution Directive (2014)	• Ensure continuity of bank's and maintaining financial stability by: i/ requiring banks to prepare recovery plans to overcome financial distress; ii/ restoring viability of parts or all of the bank. • Grant national authorities powers to ensure an orderly resolution of failing banks with minimal costs for taxpayers.
	Bank of England (BoE) - Recovery and Resolution Planning (2013)	• Ensure continuity of bank's and maintaining financial stability by: i/ requiring banks to prepare recovery plans to overcome financial distress; ii/ restoring viability of parts or all of the bank. • Grant national authorities powers to ensure an orderly resolution of failing banks with minimal costs for taxpayers.
	Federal Review Board (FRB) – Resolution Plan requirement under Regulation QQ (November 2011)	• Ensure the resilience and resolvability of globally systemic important banks (G-SIBs) without interruptions to the banks' critical operations and economic functions.... in a manner that substantially mitigates the risk that the failure of the bank would have serious adverse effects on financial stability
	IAIS – Application Paper on Recovery Planning (November 2019)	• Addresses governance, elements of a recovery plan and supervisory considerations, with an overarching focus on proportionality. The objective of a recovery plan should be to aid the insurer in understanding its own risks from a severe stress scenario and to be better prepared with an effective response and ensure timely activation and implementation of that response.
	FSB – Key Attributes Assessment Methodology for the Insurance Sector (August 2020)	• Provides a methodology for assessing the implementation of the Key Attributes of Effective Resolution Regimes for financial institutions in the insurance sector and applies to any insurer that could be systemically significant or critical if it fails (i.e. where the failure of the insurer could lead to a disruption of services critical for the functioning of the financial system or the real economy). • The methodology is intended to be used primarily in assessments performed by authorities of the existing resolution regimes in their jurisdictions, in peer reviews and in IMF and World Bank assessments, including through Financial Sector Assessment Programs.