Bank of England and FCA Discussion Paper on "Building the UK financial sector's operational resilience"

5th October, 2018

HONG KONG, LONDON and WASHINGTON – The Global Financial Markets Association (GFMA) welcomes the Bank of England and Financial Conduct Authority Discussion Paper on "Building the UK financial sector's operational resilience".

The Global Financial Markets Association (GFMA[1]) welcomes this initiative by the Bank of England and Financial Conduct Authority (e.g. "UK's financial services authorities", thereafter) to support the financial services industry in developing an approach that aims to achieve stronger operational resilience of the financial system, it's firms, FMI's (Financial Market Infrastructures) and other relevant stakeholders.

GFMA believes the focus on operational resilience will continue to increase in importance based on emerging technological change and increased global cyber threats. Achieving a more resilient financial system will require increased coordination and collaboration between different actors and jurisdictions and ensure global consistency.

GFMA welcome the initiative to provide the following comments in response to questions posed by the UK's financial services authorities in its **Discussion Paper on "Building the UK financial sector operational resilience"**.

I. General comments

Executive Summary

The GFMA welcomes, as a positive step forward, the UK's financial services authorities initiative to foster an industry dialogue with global regulatory and supervisory stakeholders on their approach to operational resilience. In particular the acknowledgement of the changing threat landscape of potential operational disruption in the future and how financial service firms can prepare in advance.

The GFMA welcomes, where relevant, that any operational resilience developments align with internationally recognised frameworks such as the CPMI-IOSCO Principles for Financial Market Infrastructures[2], the G7 Fundamental Elements of

[1] The Global Financial Markets Association (GFMA) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.

[2] https://www.bis.org/cpmi/publ/d101a.pdf

Cybersecurity for the Financial Sector[3], the NIST Cybersecurity Framework[4], ISO 22301[5], the Business Continuity Institute (BCI) Good Practices Guidelines 2018[6]. As the pace of technological change and risk of global cybersecurity threats increases, there is the potential for new frameworks to emerge that could lead to further fragmentation in approaches and increased complexity for firms and the wider-industry to respond. It will therefore be important for any framework to be harmonised at an international level, through the Basel Committee or the Financial Stability Board (e.g. FSB), to allow for common and mutually recognisable approaches to operational resilience.

GFMA believes that it is through increased cooperation and international engagement that the UK's financial services authorities can promote a globally consistent approach to operational resilience. This will ensure that any development on operational resilience relate to concepts and approaches already developed, by financial services firms that have stemmed from 9/11 and post-crisis regulatory requirements and frameworks. For example, operational continuity (e.g. the FCA's Business Recovery and Resolution Directive, the SRB's Resolution Planning), business continuity planning (BCP), business impact analysis (BIA), crisis management or cybersecurity. As a result, this would ensure any approach to operational resilience would form an extension of what has already been established and addressed to date.

However, the GFMA believes there are key areas that will require further clarification or development for an approach on operational resilience to be developed in a globally consistent manner. These are:

- To remain flexible in design and readily applicable to existing firms' structures (e.g. business models, risk appetites, existing regulatory requirements) any approach to operational resilience should be firm led;
- The maturity of operational resilience approaches should be proportionate to firms' type, size and complexity of business operations (e.g. customers, counterparties, products, trading venues, market interconnectedness);
- Further clarity on terms and concepts relating to operational resilience, which should be firm led, and how these relate to other areas such as cyber resilience and business continuity, their differences, interconnectedness and practical implications, to ensure a globally consistent approach is developed from what has already been implemented to date (e.g. business services, economic functions (or CEF), vital services, critical functions). For example, this could be achieved by a lexicon of terms related to operational resilience;
- The need to define foundational concepts such as, "business services" and "impact tolerance", how these should be derived to promote consistency within the industry, and how they will relate to any future stress-testing, which should be firm led, rather than regulatory driven;
- The extent to which services provided by firms (e.g. business services) can be aggregated or rolled up at legal entity level, across business lines and geographies to capture existing business processes, criticality levels, impact tolerances and other impact assessment data (e.g. financial consequence over time, through existing BCP or BIA studies); and
- The requirements for industry-wide metrics to provide measures of operational resilience which may be dependent on a specific type of disruption or target end-state.

While concepts of operational resilience are understood by financial services firms, for example when undergoing a system outage or a cybersecurity threat, there is no single agreed approach or set of terms. GFMA believes that to achieve an industry-wide framework for operational resilience the consultation, input and collaboration from a broad set of stakeholders and industry bodies will be required, potentially in the form of industry led workshops, facilitated by authorities.

Finally, GFMA recommends any operational resilience approach developed should have clear regulatory and supervisory expectations for firms, flexibility on how requirements can be implemented firm-to-firm against existing risk management frameworks and sufficient time for implementation.

[3] http://www.g7.utoronto.ca/finance/171013-fundamentals.html
[4] https://www.nist.gov/cyberframework
[5] https://www.iso.org/news/2012/06/Ref1602.html
[6] https://www.thebci.org/resource/good-practice-guidelines--2018-edition-.html

II. Response to questions

A: What are readers' views on the proposed focus on continuity of business services? Would a service rather than systems-based approach represent a significant change for firms and FMIs compared with existing practice? What other approaches could be considered?

The GFMA believes the proposed focus on continuity of business service for operational resilience is appropriate.

However, there should be acknowledgment that changing from a system-based to a service-based approach would be a significant change for financial service firms based on stakeholder's effort required to agree on common definitions, complete the mapping required, within an industry-wide and globally applicable context. For example:

- The lack of clarify at an industry level of what constitutes a "business services" as a foundational concept of operational resilience. This will require further engagement on what constitutes acceptable terms and concepts, which should be firm led;
- The need to obtain consensus on what constitutes a "business service" that considers diverging views and requirements depending on each stakeholder group in the industry (such as global firms, regional firms, FinTech, third-party providers or FMI's) or their discreet functions (such as technology, operations, compliance or risk) so that a consistent approach can be developed; and
- The need for financial services firms to roll up or aggregate at a "business service" level various existing business processes, which may support multiple business services, and mapping them to economic functions acknowledging that build out will be required of firms.

The scale and effort required to adapt to the proposed approach will depend on how broadly the final scope is, how "vital business services" are defined and the number of services needing capture. GFMA recommends further engagement and collaboration with industry participants, to ensure a common terminology, understanding of business services and level setting is achieved. This would allow firms to identify more clearly the differences and interrelations between the proposed approach and practices currently in place.

Finally, a number of challenges will need to be solved with a service-based approach to operational resilience. In particular:

- An end-to-end service suggests a service owner who would need to have cross-divisional/regional accountability which may not currently exist in all business areas;
- The cross-jurisdictional nature of "business services" activities could increase the complexity of operational resilience implementation; and
- The need for a balanced approach due to the dependencies of systems supporting several vital services, spread across different geographies and actors, requiring granular oversight by each firm but as a shared responsibility.

B: Would encouraging firms and FMIs to consider their contribution to the vital services that the real economy demands change the way they manage operational resilience, and if so how? What additional costs would this incur?

GFMA notes that business services supporting Critical Economic Functions (e.g. CEF) are already recognised as a high priority in systemic firms' resiliency strategies, and "critical services" have been agreed with regulators as part of existing regulatory requirements such as Group Resolution Plans. To the extent to which an approach on operational resolution is developed, it will need to align and build on the aforementioned existing practices on operational resolution where they are already in place (systemic firms, GSIBs), in addition to existing firms' business resilience practices.

Encouraging firms to consider their contribution to the vital services that the real economy demands (e.g. economic functions) will also require:

- Mapping "business service" to economic functions, as well as underlying dependencies;
- Testing resilience at an aggregate level (e.g. legal entity) and providing adequate evidence; and
- Achieving industry-wide consensus and potentially involving other jurisdictions or sectors, such as systemically important third parties, on which financial service firms may have dependencies.

The change will incur additional costs relating to:

- The clarification of foundational concepts (e.g. "business services", "impact tolerances") and how these compare with other relevant regulatory concepts ensuring a consistent approach is developed (e.g. cyber resilience, business continuity);
- The mapping of business services to economic functions and underlying dependencies (e.g. systems, people, processes);

- Obtaining consensus from a wide range of stakeholders whom may have different views depending on each industry stakeholder group (e.g. global firms, regional firms, FinTechs and third-party providers, FMI's) or discreet function (e.g. technology, operations, compliance, risk) to achieve an industry-wide consistent approach;
- Implementing the agreed approach gradually and with sufficient flexibility for each firm to accomplish the transformations required within firm's existing risk management frameworks and change portfolio;
- Identifying metrics to track and measure operational resilience information; and
- On-going learning and developing of operational resilience.

C: How do boards and senior management currently prioritise their work on operational resilience?

Currently boards and senior management prioritise their work on operational resilience by having direct reporting lines with their senior management and SME's, receiving activity reporting when relevant or when a situation arises requiring their involvement or decision. For instance, a board risk committee could be constituted to provide an independent challenge to the board on risk management considerations and operational risks.

When relevant, board and senior managers may be involved in activities related to:

- Business Continuity Management;
- Crisis Management and relevant crisis simulations;
- Business Impact Analysis and/or Business Environment Assessments;
- Enterprise Risk setting;
- Recovery and Resolution planning; and
- Cybersecurity.

GFMA believes it is important, here, to make a key distinction between the role and responsibilities of the Board and Senior Managers in relation to operational resilience. While it is expected for the Board to set the firm's strategy and risk, the level of detail required to set business service impact tolerances, is typically the responsibility of Senior Managers. GFMA recommends authorities to consider that a firm's Board should have adequate access to expertise and resources, such as Senior Managers, which can provide such expertise.

D: What changes are firms and FMIs planning to make to strengthen operational resilience over the next few years? How involved are board members in the planning, implementation and embedding of any changes? What are the likely benefits and costs involved?

Financial services firms will continue to strengthen their operational resilience across several related areas. These include:

- Governance and culture;
- Skills and resources;
- Implementation of operational resilience programs;
- On-going monitoring and reporting;
- Scenario testing; and
- Learning and developing.

It can be expected that financial services Boards, as appropriate, will be required to be involved in a number of initiatives related to these areas.

GFMA believes the likely benefits and costs of increased operational resilience as suggested by the UK's financial services authorities to be:

- The overall benefit of increased operational resilience of firms and to the economy through increased financial stability.
- The overall scale, cost of design and implementation of an approach to operational resilience, with could diverge from existing firms' structure in place, the risk of fragmented approaches developed in jurisdictions and upcoming supervisory requirements.

E: What are readers' views on the possibility of firms and FMIs being asked to set impact tolerances for their most important business services?

GFMA believes that asking firms to set "impact tolerances" for their most important business services could be helpful to mature operational resilience across the industry and should remain aspirational rather than to meet supervisory expectations. This would provide the right level of incentives for firms and regulators to foster a dialogue on operational resilience, to increase the overall level of effort required, rather than crystallising impact tolerances as a hard and fast rule. As an example, setting an RTO for a malicious cyber-attack would have to take account of the wide variance for the time it could take to establish whether an attack has occurred and how pervasive and extensive the attack could be. Indeed, Bank of International Settlements (BIS), in its white paper aimed at enhancing regulatory approaches to cyber-security, comments[7] "*mandating a specific recovery time is another example where regulators need to be careful how banks go about implementing it. The aim is to prevent the lengthy disruption of critical financial operations, but an excessively stringent and rigid recovery time may prove counterproductive if it comes at the expense of the bank's ability to check its systems are no longer compromised*". Once a mapping of applications and processes to "vital business services" has been complete, it is understood that it should be possible to re-purpose existing metrics and reporting documents to meet regulatory expectations, including generating impact tolerances for relevant services.

However, further clarity and consensus is required on the definition and method of applying "impact tolerances" as an important foundational concept of operational resilience. For example, this would include:

- Defining "impact tolerances" as a foundational concept of operational resilience with an industry agreed definition and description;
- The UK Financial Services Authorities may consider further engagement and collaboration with industry participants, to support industry led guidance on "impact tolerances", providing greater clarity on: supervisory expectations of firms, how to define "impact tolerances" and how "impact tolerances" feed into existing frameworks and practices such as risk appetites, business continuity, Recovery Time Objectives (RTOs);
- Obtaining consensus on what constitutes an "impact tolerance" from a broad set of stakeholders. However, this could be challenging due to the different types of disruptions (e.g. which could lead to different tolerances), and the potentially diverging views on the meaning of terms depending on each stakeholder group in the industry (e.g. global firms, regional firms, FinTechs and third-party providers, FMI's) or discreet function (e.g. technology, operations, compliance, risk);
- Alignment and close cooperation within firms will be required to set firm-wide "impact tolerance levels" and go beyond regulatory compliance (e.g. level setting and reporting), to identify concrete actions required to enhance firms' resilience posture. GFMA anticipates setting tolerance levels could have more far-reaching implications, as it may require alignment with firms' client obligations and product Service Level Agreements (SLAs);
- Aggregating "impact tolerances", across various existing business processes captured by financial services firms today, using business criticality and other assessment data (e.g. financial consequence over time, through existing BCP or BIA studies), and mapping these to the economic functions provided;
- Planning for plausible disruption scenarios or target end states would support firms' efforts in identifying solutions or preferred containment options, including transition periods. GFMA believes firms and regulators should work collaboratively to identify disruption types and relevant criteria to measure their severity and potential impact on firms. However, while this identification would provide further clarity to firms and regulators, it may not be desirable to devise impact tolerances that measure all possible outages in a comparable way. We recommend sub-categorising extreme events (e.g. "black-swan"), such as a large-scale cyber-attack, where impact tolerances in such events could potentially be so severe, it would be difficult to compare with other types of disruptions. Indeed, cybersecurity attacks pose unique challenges due to yet unknow information at the time of the attack (e.g. starting point, promulgation methods, malware properties, remediation mechanism) and therefore, should not form part of hard and fast rules. A sustained good governance model would be safer and more efficient in over-coming the constantly evolving nature of cyber threats, notwithstanding potential data corruption or contagion risks to the wider financial eco-system; and
- Potential substitutability options identified at a theoretical level may be more complex and resource intensive in reality.

Based on these challenges, the GFMA recommends the UK Financial Services Authorities focus on developing an approach that aims to increase the maturity of operational resilience within firms as its primary objective, rather than a supervisory assessment tool.

F: What approach and metrics do firms and FMIs currently use?

[7] Regulatory Approaches to Enhance Bank Cybersecurity Frameworks", August 2017, (p.10), link

Currently firms use:

- An approach based on existing capabilities such as operational continuity (e.g. the FCA's Business Recovery and Resolution Directive, the SRB's Resolution Planning), business continuity planning (BCP), business impact analysis (BIA). Crisis management or preparedness against cyber-attacks also allow for an understanding of a financial services firm's resilience under certain disruptions or stress scenarios; and
- Metrics which relate to the understanding of business processes on business criticality, impact tolerances and other impact assessment data and how these compare with metrics from third party providers (e.g. financial consequence over time, through existing BCP or BIA studies).

G: If these proposals would require some firms and FMIs to update part of their existing risk management framework, what would this involve?

The proposal of the UK Financial Services Authorities would require firms to produce a detailed end-to-end mapping of processes, applications and people, which would represent a significant effort to develop and maintain. Identification and prioritizing of "Vital Business Services" driven by first line of defence would require effort to update policies, standards and procedures and associated management information tools including KRIs, KCIs and KPIs. In addition, the testing and exercising of operational resilience programs would entail significant effort of firms depending on their frequency, scale and level of integration required (e.g. across different business units and geographies).

Firms would need to assess the impact in aggregate, on:

- Governance and culture;
- Skills and resources;
- Implementation of operational resilience programs across business lines and geographies (e.g. exposure identification, quantification of risk exposure, establishing policies and procedures on how to manage points of failure in line with a firm's enterprise risk management framework (e.g. risk appetite), identify and execute strategies to manage risks) and it's testing or exercising: (e.g. executing strategies);
- On-going monitoring and reporting (e.g. monitoring exposures); and
- Learning and developing: (e.g. continuous improvement).

Updating parts of firms' risk management framework will largely dependent on the degree of overlap or divergence between current practices in place and the proposed approach. To provide more clarity to firms, GFMA recommends authorities to address the following two areas of ambiguity:

- The scope of "vital business services", and the extent of overlap between these services and Critical Economic Functions (CEFs) as defined for resolution planning purposes and already captured by "critical business processes" mapping; and
- The differences (or otherwise) between metrics currently used to calculate "critical business processes" (e.g. KCIs, KRIs, RTO, etc.) and the authorities' conception of "impact tolerances", and the extent to which existing metrics can be repurposed to meet regulatory expectations.

H: What are readers' views on producing an impact tolerance statement as described? What relevant operational resilience risk management documentation do firms and FMIs already produce, and how does this differ from impact tolerance statements?

GFMA views the production of an impact tolerance statement as a useful step to mature industry and regulatory stakeholder's approach to operational resilience.

Currently firms and FMIs produce relevant operational resilience risk management documentation related to: Operational continuity (e.g. the FCA's Business Recovery and Resolution Directive, the SRB's Resolution Planning), business continuity planning (BCP), Business Impact Analysis (BIA) crisis management, cybersecurity and various existing business processes captured by firms today on business criticality and impact assessment data.

However, these differ from impact tolerance statements because:

- Impact tolerances for disruption are expected to be set for the most important "business services", on which an industry wide consensus may be challenging to achieve, as per responses to questions A) and B);

- Impact tolerance are expected to describe a firm's tolerance for a disruption to a particular business service, under the assumption that disruption to the systems and processes supporting that service will occur. However, achieving an industry-wide consensus on a certain level of "impact tolerance" may be challenging to achieve, due to the potentially diverging views on what is an acceptable business disruption, depending on the nature of the disruption, the view point of each stakeholder group in the industry (e.g. global firms, regional firms, FinTechs and third-party providers, FMI's) or discreet functions (e.g. technology, operations, compliance, risk);
- Impact tolerances are expected to express reference to specific outcomes and metrics for processes and systems (e.g. metrics such as maximum tolerable duration or volume of disruption, measure of data integrity, number of customers affected). However, for these metrics to describe the state of operational resilience of firms and the industry, consistency will be key to ensure similar standards are applied. GFMA believes this may be challenging to achieve due to the dependency of metrics on the nature of the disruption, scenario, plausibility, scale, and complexity;
- Supervisory authorities are considering setting their own impact tolerances which may diverge from what industry has considered; and
- Impact tolerances will require a globally coordination approach to avoid different jurisdictions developing and applying their own standards and metrics and the potential involvement of other jurisdictions and sectors, such as systemically important third parties, on which financial service firms may have dependencies.

I: What operational resilience tests or scenarios do firms and FMIs already consider and undertake for their own risk management purposes? What factors do firms and FMIs take into account when devising operational resilience tests or scenarios?

For their own risk management purposes financial services firms consider and undertake a number of operational resilience tests or scenarios. For example:

- Preparing for Operational Disruption;
- Business continuity planning (BCP) & Testing;
- Crisis Management Plan & Exercising;
- Cybersecurity (e.g. penetration testing, cyber-attack simulations such as table-top exercises or cyber range exercise); and
- Risk management approach for Business transformation Programs.

Financial services firms take into account a range of factors when devising operational resilience tests or scenarios. For example:

- Operational continuity (e.g. occurrence of a recovery or resolution event);
- Contingencies (e.g. events which could lead to a disruptive and unexpected event that threatens to harm the firm or its stakeholders);
- Crisis (e.g. events which could lead to a severely disruptive and unexpected event that threatens to harm the firm or its stakeholders);
- Cyber-threats; and
- Business Transformation Programs.

On the development of resilience tests GFMA believes:

- Further clarity should be provided to firms on how potential resilience tests would be completed and run and implications for firm's supervisory assessments;
- Any framework on operational resilience should be managed, implemented and tested by firms with adequate guidance and support from regulators for attestation;
- The testing and exercising of operational resilience programs would entail significant effort of firms depending on their frequency, scale and level of integration required (e.g. across different business units and geographies).

J: How do boards and senior management currently gain assurance over the operational resilience of their firm or FMI?

Boards and senior management gain assurance over the promotion of operational resilience of their firms by established methods and ways to measure their effectiveness in use by the industry today. For example, these include:

- Implementation of operational resilience programs (e.g. Business Continuity and Disaster Recovery testing);
- Scenario testing (e.g. table top exercises for different operational and cyber events and scenario analysis workshops for extreme but plausible events);
- On-going monitoring and reporting; and
- Training and developing programs.

Operational resiliency includes the activities to prevent operational disruptions. Therefore, boards and senior management also receive regular updates on the cybersecurity risk management program activities and strategy. Given the evolving threat landscape, new/emerging technology solutions and maturing regulatory landscape, the oversight of cybersecurity resiliency efforts have increased oversight from these governance bodies.

K: What are readers' views on the proposed developments to the supervisory authorities' approach to operational resilience?

GFMA believes the UK's financial services authorities approach to operational resilience is a positive initiative on commencing a dialogue with the industry on an approach to increase operational resilience and financial stability.

However, as per our response to the questions posed in this discussion paper, we believe that clarification of the points listed below is required:

- A common approach and framework that can be applied consistently and proportionately across different financial services stakeholders, functions and jurisdictions;
- Further clarity on foundational definitions such as "business services" and "impact tolerances", which should be firm led;
- The use of existing operational resilience approaches to prevent further fragmentation or complexity in its application across the industry; and
- Clarifying expectations on firms.

In addition to our answers provided on each question above, GFMA wishes to highlight the following considerations:

- GFMA supports a principle-based approach that can be applied to the different kinds of disruptions that will need to be considered under the proposed framework and would encourage authorities to build in an appropriate amount of flexibility. For example, impact tolerance and RTOs for a certain business service will be different in a market-wide severe stress scenario than under a firm-specific outage scenario, driven by differences in ability to recover that may be beyond one firm's control.
- GFMA acknowledges the increased regulatory focus on outsourcing services across jurisdictions, but would urge regulators to recognise that a robust framework exists today for managing and overseeing inter-affiliate service and advisory support relationships:
    - Firms' outsourcing models are linked to global operating models, and analysis are performed by second and third line of defence between the outcomes of onsite delivery versus outsourcing of relevant functions; and
    - Authorities' expectations should be based on what is practically achievable in terms of third-party providers oversight, in particular when relating to stress-testing, and the existence of currently in place contractual relations.

GFMA recommends authorities to consider not introducing addition requirements that could disrupt the operating model of global firms and could create inefficiencies.

GFMA recommends greater international coordination to ensure a global approach is devised and fits with on-going international initiatives to harmonise cyber security and resilience (e.g. FSB Cyber Lexicon, BCBS ORG).

Contacts

GFMA	Alison Parent	+1 (202) 962-7393	aparent@gfma.org
AFME	Emmanuel Le Marois	+44 (0)20 3828 2761	emmanuel.lemarois@afme.eu
AFME	David Ostojitsch	+44 (0)20 3828 2761	david.ostojitsch@afme.eu
SIFMA	Tom Wagner	+1 (212) 313 1161	twagner@sifma.org
ASIFMA	Laurence Van der Loo	+852 2531 6500	lvanderloo@asifma.org

About GFMA

The Global Financial Markets Association (GFMA) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.