BCBS Operational Resilience Group: GFMA Outreach

Outreach Meeting, London, 27th September, 2018

HONG KONG, LONDON and WASHINGTON – The Global Financial Markets Association (GFMA) welcomes the initiative by the Basel Committee to set a "Operational Resilience Group (ORG)".

The Global Financial Markets Association (GFMA[1]) welcomes the initiative by the Basel Committee to setup an "Operational Resilience Group (ORG)" to support the financial services industry in achieving a stronger operational resilience of the financial system, its firms, FMI's and other relevant stakeholders.

GFMA believes the focus on achieving operational resilience will 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 across jurisdictions.

GFMA welcome the invitation to provide the following comments in response to questions posed by the Basel Committee on Banking Supervision (BCBS) in preparation of the Outreach Meeting in London, 27th September 2018.

I. General comments

Executive Summary

The GFMA welcomes as a positive step forward the Basel Committee's initiative, in line with the Bank of England and FCA's (e.g. "UK's Financial Services Authorities" thereafter) Discussion Paper "Building the UK financial sector's operational resilience", 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, the G7 Fundamental Elements of Cybersecurity for the Financial Sector and the NIST Cybersecurity Framework . 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 BCBS or the FSB, to allow for international consistency and for common and mutually recognised approaches on operational resilience.

[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.

GFMA believes that it is through cooperation and international engagement that the BCBS can promote a dialogue on how to align with the UK's Financial Services Authorities approach. This will ensure that any development on operational resilience relate to concepts and approaches already developed by financial services firms that have stemmed from post-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), operational continuity in resolution (OCIR), 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 and readily applicable to existing firms' structures (e.g. business models, risk appetites), any approach to operational resilience should be firm led;
- 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", and 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;
- 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 jurisdictions, 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 event or target end-state.

While concepts of operational resilience are understood by financial services firms, for example when undergoing a resolution event or a cybersecurity threat, there is no single agreed approach or set of terms linking back to operational resilience. The 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 workshops.

Finally, the 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.

II. Response to questions

a. Session 1: Overview of the range of existing expectations and practices on cyber resilience

GFMA believes that Business Continuity Management (BCM) and cyber security both aim to increase a firm's resilience, preparedness and response to a potential crisis. However, from an organisational perspective cyber security is considered an IT issue that could become a crisis, while BCM relates to the planning of a crisis or disaster.

Therefor any approach to operation resilience will require the alignment of these areas (e.g. cybersecurity and BCM), which presents organisational complexities, and in addition will require an aggregated view of a firm's state of resilience across multiple dimensions (e.g. business lines, jurisdictions, third party dependencies).

Q1: What are the unique challenges in governance of cyber risks (compared to broader operational risks)?

GFMA believes the unique challenge of cyber risk governance is the confidentiality, availability and integrity of data and systems, due to the potential corruption and destruction of a firm's vital data. GFMA believes that because of this unique aspect cyber security risks require specific considerations compared to traditional operational risks.

Considerations include:

- **Detection**: Unlike kinetic disruptions (such as a loss of power, loss of location, etc.), which as a technical matter is immediately apparent and limited to a defined sphere, cybersecurity attacks are often difficult to detect or diagnose and frequently pose a risk of contagion to other systems or the market at large. Additional time is required for investigating the actual cause of the operational impact and then testing and validating systems after the attack to ensure that the systems are ready for safe operation;
- **Response**: Given the unique characteristics of a cyber-attack, the ability to recover business operations and ensure that the environment is safe to reconnect to the financial ecosystem within a 2-hour time period may increase the contagion risk of a significant cyber-attack.

This means that cyber threats may require a different response than traditional operational risks.

Typically, the Cybersecurity function within firms is the responsibility of the Chief Information Security Officer (CISO) who reports into the Chief Technology Officer (CTO) and Chief Operating Officer (COO). While Business Continuity Management (BCM) typically sits within Risk and therefor reports into the Chief Risk Officer (CRO).

Q2: How to better implement the 3 lines of defence model in order to guarantee an adequate monitoring of the cyber resilience by institutions?

GFMA believes the 3 lines of defence model is overall well understood and implemented by firms.

In summary:

- **The first line or "management control"** sits within the CISO function, who reports into the CTO and COO, and has a reporting line to the Board. The first line has responsibility of assessing asset's vulnerabilities and actively seeks to manage cyber risks within the organization's risk appetite. The first line is also tasked with handling risk events, updating key risk indicators (KRIs), and deploying and managing controls that affect people, processes and technology.
- **The second line or "risk management"** is tasked with monitoring how management is handling cyber risks. This includes:
    - Determining the extent that risks are actively monitored and appropriately managed;
    - Looking at cybersecurity control frameworks;
    - Defining KRIs and metrics;
    - Creating risk assessments, tests and conformance reviews by tracking actions of the first line; and
    - Analysing the impact of those actions to determine their effectiveness in mitigating cyber risks

- **The third line or "internal audit"** provides an independent assurance. The third line is tasked with evaluating the overall process of cyber risk governance, ensuring internal control frameworks are adequate and having the ability to challenge the first and second line where additional information or clarity is required.

While these concepts are well understood and implemented by firms, different organisational structures require a degree of flexibility on how firms implement the 3 lines of defence model.

As previously mentioned the Cybersecurity function within firms is typically the responsibility of the Chief Information Security Officer (CISO) who reports into the Chief Technology Officer (CTO) and Chief Operating Officer (COO). Business Continuity Management (BCM) typically sites within Risk and therefor reports into the Chief Risk Officer (CRO).

However, for a better management of the 3 lines defence model, GFMA believes:

- **An integrated approach** would ensure best practices and frameworks are applied consistently across the 3 lines to ensure a consistent and integrated approach is developed firm-wide;
- **Appropriate governance** (e.g. segregation of roles and responsibilities) should be observed to ensure the first line and control functions are performed by separate groups; and
- **In a rapidly changing environment individuals irrespective of their role should ensure their skills and competencies are kept abreast** of recent market and technological developments to remain relevant in their function.

Q3: The role of the CISO consistently defined and understood? What is the exact role of the Chief Information Security Officer (CISO) compared to Chief Risk Officer (CRO), and how to articulate them?

GFMA believes the role of the Chief Information Security Officer (CISO) is consistently defined and understood as a first line or 'management control' role. From an organisational perspective the CISO sits with technology and information security, and is considered a risk owner and taker, in charge with implementation.

The role of the CISO compared to the Chief Risk Officer (CRO) is understood as, the CRO is a second line role. From an organisational perspective, the CRO sits in risk, and considers the identification and mitigation of risks, which are wide ranging, including cyber.

However, due to the different organisational structure of firms, a degree of flexibility is required on how firms implement the 3 lines of defence model.

Q4: What could be the best way to address the "cyber" competencies/skills challenges that face institutions?

GFMA believes there are various ways to address the "cyber" competencies/skills challenge that institutions are facing.

These may include activities related to:

- Governance and culture;
- Skills and resources;
- Implementation of cybersecurity programs;
- On-going monitoring and reporting;
- Exercising;
- Learning and developing; and
- Partnerships.

Q5: What metrics or indicators are currently useful when discussing cyber resilience at Board level?

GFMA believes the following practices are relevant when discussing cyber resilience at Board level:

- Cybersecurity should be regularly discussed at Board level but is more appropriately and regularly discussed at the Group risk committee, which reports into the board;
- Frequency of cybersecurity board level discussions should range from every quarter to bi-annually;

- In addition to a recurring item of discussion, the board should complete deep dives, on cybersecurity selected topics when relevant, depending on forward-looking investments or risk appetite; and
- The board should aim to have presentations completed by the first line (e.g, CISO) and by second and third line (e.g. CRO) to challenge views.

Q6: Which metrics / benchmarks have proven successful in and outside the banking industry? What could be used as 'leading' or forward-looking indicators of cyber resilience?

GFMA has not provided a response to this question.

Q7: What are the practical challenges faced by banks related to the interaction with third party service providers?

GFMA views the practical challenges faced by banks relating to third party service providers interaction include:

- The potential classification of systemic third parties as critical infrastructures; however further clarify should be provided as the criteria for identification and selection, as well as potential unintended consequences. This would require a globally coordinated regulatory response to ensure a consistent approach is developed across various jurisdictions; and
- GFMA believes that in the case of large service providers, such as Cloud computing Service Providers (CSPs), pooled audits are an appropriate solution for providing assurance. For example, the European Banking Authority (EBA) in its 2017 Cloud Outsourcing Guidelines recognised pooled audits as an acceptable practice for performing access and audit rights.

Q8: What are the challenges faced by the third parties in adhering to existing banking requirements?

GFMA believes the challenges faced by third parties in adhering to existing banking requirements can be summarised under the following:

- Third parties falling outside the regulatory perimeter; and
- The ability of regulated firms to enforce requirements down to third parties by contractual requirements and vendor relationship management.

b. Session 2: Main industry concerns with regulatory fragmentation and implementation challenges in broader operational resilience, and implications for banking supervision

Q1: What are the main sources of risks and remaining regulatory / maturity gaps according to banks?

While an important and positive step forward, there needs to be acknowledgement that operational resilience is a developing area of regulatory focus and regulators and firms will have a different approach to operational resiliency.

GFMA recommends the Basel Committee to engage with jurisdictions developing an approach on operational resilience, such as the UK authorities, and foster a dialogue with other participants seeking a consistent approach on operational resilience at a global level.

GFMA recommends the Basel Committee to dedicate appropriate time and engagement, focused on understanding existing practices, including where they differ, and target areas of enhancement before introducing new requirements on a "one-size-fits-all" basis.

GFMA recognises the increased regulatory focus on outsourcing services across jurisdictions (e.g. EBA Outsourcing Guidelines2), and urges the Basel Committee to consider how greater clarity and consistency could be provided to firms when entering third-party or intra-group outsourcing arrangements in the context of operational resiliency:

- A robust framework exists today for managing and overseeing inter-affiliate service and advisory support relationships, which has been vetted and approved by regulatory authorities across the globe. Firms' outsourcing models are linked to global operating models, and analysis has been performed by second and third lines of defence between the outcomes delivered by onsite versus outsourced coverage of relevant functions.
- Where outsourcing to third-party providers is deemed appropriate, oversight of the operational resilience of those providers is still maintained and considered in assessments of the overall resilience of the firm.

Q2: What strategies, governance approaches and tools have banks found to be effective in developing and implementing a sound operational resilience framework? What are some of the emerging practices in the field?

GFMA notes that business services supporting Critical Economic Functions (e.g. CEF) are already recognised as a high priority in firms' resiliency strategies as part of Group Resolution Plans.

In addition, we believe Operational Continuity in Resolution (e.g. OCIR) provides the foundation for coverage of broader resiliency scenarios.

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, in addition to existing firms' business resilience practices.

Q3: Have banks used and learnt lessons for their implementation of the Basel Principles on ebanking and on sound management of operational risks?

GFMA has not provided a response to this question.

Q4: Are there concrete instances of regulatory fragmentation (geographical, sectoral) where the addition of requirements actually weakens institutions' operational resilience, produces most significant overheads, and what could be done to address the issues?

GFMA notes the following regulatory development and potential impact on operational resilience:

- The increased regulatory focus on outsourcing services across jurisdictions such as the EBA's Outsourcing Guidelines3 impacting third-party or intra-group outsourcing arrangements and related data transfers;
- Structural reform (or Ring-fencing)[4];

[2] EBA Consults on Guidelines on Outsourcing (link)
[3] EBA Consults on Guidelines on Outsourcing (link)
[4] https://www.bankofengland.co.uk/prudential-regulation/key-initiatives/structural-reform

- Bank Recovery and Resolution Directive (BRRD)5;
- Balkanisation of data localisation requirements due to certain jurisdictions; and
- The lack of coordination across geographies on testing requirements resulting in an inefficient use of firms' resources, shifting away from enhancing firms' processes to satisfying regulatory expectations.

Business services supporting Critical Economic Functions (e.g. CEF) are already recognised as a high priority in firms' resiliency strategies as part of Group Resolution Plans.

In addition, we believe Operational Continuity in Resolution (e.g. OCIR) provides the foundation for coverage of broader resiliency scenarios.

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, in addition to existing firms' business resilience practices.

Q5: Is there a set of high-level principles or an existing international scheme that would form an adequate basis for further policy elaboration by the Basel Committee?

GFMA notes to following high level principles on any approach to operational resilience:

- Over-arching international dialogues to foster mutual recognition of standards, so that any approach developed in a specific region (e.g. UK supervisors) is consistently understood and applied globally;
- Flexibility in design to be readily applicable to firms' currently existing structures, recognising there is 'no one size fits all'. This would be more easily achieved if the initiative was firm led and facilitated by relevant regulatory stakeholders; and
- Recognition of currently existing standards and requirements which have been implemented by firms to date, and how an approach would build on this basis.

GFMA invites the Basel Committee to reference on the existing international scheme developed by the International Organization for Standardization (ISO) on establishing a technical committee (TC 292) on security and resilience.

- As part of its work, ISO TC 292 has established various working groups, including business continuity management, incident management, organizational resilience and supply chain security. The ISO published a standard on "Organizational resilience – principles and attributes" (ISO 22316:2017) in May 2017.
- In regard to ISO 22316:2017, the convenor of the ISO TC 292 working group that developed the standard stated: "The standard [ISO 22316:2017] takes a wide view of the things that can drive resilience in an organization; many of these are behavioural and have historically been overlooked. This is why one of the key principles of the standard is to help them develop a culture that supports resilience. It also involves building upon existing forms of risk management, having shared values and an awareness of changing contexts, all the while underpinned by strong and empowered leadership."
- One of the objectives of ISO 22316:2017 is not only to help organisations be better placed for anticipating and responding to potential risks, but to help future-proof business activities and to enable organisations to harness opportunities. The standard is designed to be used throughout an organisation's life cycle, and it does not promote uniformity in approach across all organisations, as specific objectives and initiatives are tailored to suit an individual organisation's needs.

Q6: How are firms working with key stakeholders within their eco-system to enhance operational resilience?

GFMA has not provided a response to this question.

Q7: How could testing and assurance methodologies be further improved?

GFMA has not provided a response to this question.

[5]https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/managing-risks-banks-and-financial-institutions/bank-recovery-and-resolution_en

Contacts

GFMA	Alison Parent	+1 (202) 962-7393	aparent@gfma.org
AFME	Emmanuel Le Marois	+44 (0)20 3828 2761	emmanuel.lemarois@afme.eu
SIFMA	Tom Wagner	+1 (212) 313 1161	twagner@sifma.org
ASIFMA	Laurence	+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.