5th October 2018

Jack Armstrong (Bank of England), Jon Newton (PRA) and Chris Walmsley (FCA)
Bank of England
Threadneedle Street
London, EC2R 8AH

Via Electronic Submission

Re. BANK OF ENGLAND AND FINANCIAL CONDUCT AUTHORITY DISCUSSION PAPER ON BUILDING THE UK FINANCIAL SECTOR'S OPERATIONAL RESILIENCE

Executive Summary

- FIA[1] supports the key objectives of the proposals in the Discussion Paper, namely to promote business continuity and to maintain confidence within the financial sector in the event of a disruption to services. FIA submits this on behalf of its clearing members that are critical providers within the overall clearing ecosystem. Any consideration of operational resilience should consider the integrated nature of the service providers within the clearing market infrastructure.

- Business services should not be considered in isolation; for example, where an emphasis may be placed on FMIs to continue providing clearing services, they can only do so when clearing members are also able to provide their services as well and supporting infrastructure such as payments systems remain resilient. Where an institution may provide multiple business services, services that are important to maintaining a portion of the financial sector should be prioritised even if they

[1] FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in Brussels, London, Singapore and Washington, D.C. FIA's membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from more than 48 countries as well as technology vendors, lawyers and other professionals serving the industry. FIA's mission is to support open, transparent, and competitive markets; protect and enhance the integrity of the financial system; and promote high standards of professional conduct. As the principal members of derivatives clearinghouses worldwide, FIA's member firms play a critical role in the reduction of systemic risk in global financial markets. Further information is available at www.fia.org.

are relatively small parts of a global financial institution; this is a concept highlighted by the PRA's approach to Critical Economic Functions (CEFs).[2]

- Operational resilience responsibilities should be principles-based and encourage private/public partnership to allow processes to evolve as changes occur within the financial sector; public/private coordination is important for information sharing regarding innovation, threats and hazards, and key to the development of playbooks that can be utilized by both regulators and industry participants in the event of disruption.
- FIA encourages the UK supervisory authorities to engage closely with the industry to understand existing practices, including where they differ across firms and industries within the financial sector to ensure that the operational resilience requirements remain principles-based and appropriately proportionate to the size and type of firm.
- Proportionality is key to ensuring appropriate systems, resources and procedures are implemented; there should not be a one-size-fits-all approach that becomes a high barrier to compliance. As such, impact tolerances should be set according to a firm's assessment of its own business services in the context of the broader industry.
- Cyber security and cyber resilience should not be treated separately from broader operational resilience since technology is at the heart of most business services within today's interconnected markets.
- Increased outsourcing of both technology and services allows firms to maintain operational efficiency yet presents challenges for firms to comply with strict operational resilience requirements; as such, requirements should focus on the governance and risk management of outsourced technology and services rather than imposing strict compliance requirements.
- Continued evolution of technology presents both opportunities and challenges, with risk management key to ensuring resilience without stifling innovation, both for new technology (for example "fintech"), as well as changes to existing technology; as such we support the idea of principles-based minimum standards for new entrants to establish themselves within a market without compromising its integrity or resilience.
- Governance around operational resilience should be harmonised across regulatory regimes to avoid the creation of conflicting requirements and regulatory firewalls within global financial institutions that provide multiple business services, not just in the UK but also internationally. Harmonisation should include the adoption of standard lexicons of operational resilience terms and common understanding of operational resilience principles across major jurisdictions.

[2] BoE Supervisory Statement | SS19/13 Resolution planning, December 2013, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2015/ss1913-update.pdf

Introduction

FIA welcomes the opportunity to respond at this early stage to the Bank of England, Prudential Regulation Authority and Financial Conduct Authority's (collectively the "UK supervisory authorities") Discussion Paper on building the UK financial systems operational resilience ("the Paper").

The cleared derivatives industry is a key part of the wider financial sector within the UK and is a global industry that facilitates the transfer of risk between international entities utilising financial market infrastructure (FMI) both within and outside the UK.

FIA has been an active proponent of cybersecurity[3] and operational resilience within the cleared derivatives industry for many years, most notably through its organisation of annual disaster recovery testing within the industry[4] and its cyber resiliency workshops.[5]

FIA is supportive of the Paper's focus on *building* operational resilience, especially the emphasis on continuity of business services in the event of a disruption to the financial sector (which may be localized in impact or widespread, dependent upon the type of incident), and believes that the approach set out in the Paper will be an expansion of firms' current practices but not a major departure from how the industry addresses operational resilience today.

Since this is a developing area of regulatory focus, firms will have different approaches to operational resilience. As such, FIA strongly encourages the UK supervisory authorities to dedicate further time to engage closely with the industry to understand existing practices -- including where they differ across firms and sub-sectors within the financial sector to ensure that requirements remain principles-based and appropriately proportionate to the size and type of firm.

Public / Private partnership and common approaches to operational resilience

FIA believes that principles around operational resilience should be developed through a robust public/private dialogue so that regulators understand both the pros and cons of the adoption of technology and create principled-based regulation accordingly that allows continued innovation and evolution, yet within the appropriate framework for managing the risks presented.

Much regulatory focus has recently been placed on cyber security standards or principles around fintech. Within an ever increasingly technology-driven financial sector, such work should be cross-referenced as part of harmonised operational resilience – for example the concept of sandboxes and/or information

[3] In the United States, FIA is a member of the Financial Services Sector Coordinating Council (FSSCC), the Financial Services Information Sharing and Advisory Center (FS-ISAC) and participates in regular public/private sector discussions on cyber security with the US government's Financial Banking and Information and Infrastructure Committee (FBIIC). FIA is a stakeholder in the FSSCC initiative for regulatory harmonisation for cyber security regulation based on the National Institute of Standards and Technology (NIST) framework. FIA has also participated in the US Treasury's Hamilton Series of cyber security exercises and has worked with its members to provide business continuity-oriented workshops regarding hypothetical cyber events within the cleared derivatives industry.

[4] https://bcp.fia.org/events/2018-fia-disaster-recovery-test

[5] https://fia.org/articles/fia-market-technology-division-simulates-cyber-attack-clearinghouse

sharing are not unique to fintech, and common lexicons such as that proposed recently by the Financial Stability Board (FSB)[6] are not unique to cyber security.

FIA also advocates the development and harmonisation of financial sector specific playbooks that allow all market participants – including regulators – to follow a clearly defined action plan in the event of disruption, with clearly articulated lines of communication, escalation and coordinated resolution.[7] Such playbooks should be harmonised with other industry sectors so that recovery from localized natural events or disruption to services such as power or telecommunications can be coordinated, as well as harmonised with playbooks used in other jurisdictions in the event of non-localised events (such as a coordinated cyber attack on a global financial institution). For this work, International organisations such as CPMI-IOSCO or the FSB are well-suited to unite international regulators and the private sector to adopt a standard approach to crisis management.

Evolution of the global cleared derivatives industry

Since the financial sector covers many different types of business activities, we will focus our response on the role of the cleared derivatives industry, both within the UK itself as well as the role that UK derivatives markets and UK participants play internationally, and how the Paper should address financial market infrastructure (FMI) within this space (clearinghouses, exchanges and other key service providers such as custodians and cash and collateral management utilities) and the clearing members (CM) who facilitate the transactions on the FMIs. Indeed, we note that the Paper on Page 14 refers to a potential disruption to derivatives trading affecting the ability of firms to protect themselves against financial risk, therefore affecting market confidence and increasing the risk of default of a major market participant.

FIA believes that in today's interconnected world, technology underpins the financial sector and is the main facilitator of global access to many markets, but especially global exchange traded derivatives. The increased adoption of technology within the financial sector over the last 25 years has led to unparalleled levels of growth in global transaction volumes for cleared derivatives, especially with the establishment of electronic exchanges and clearinghouses that facilitate transactions across all time zones.

FIA agrees with the premise in section 1.5 of the Paper that disruption can come in many forms as summarised in Figure 1 of the Paper. Technology within financial services has evolved and will continue to do so at a faster rate than before. This evolution will include many innovative or disruptive approaches to traditional processes. We increasingly see this in what has been termed "fintech", where non-traditional financial services providers are entering the market and disrupting the *status quo* through their introduction of new technology. As the Paper notes, evolution not only brings new opportunities but also presents new challenges, particularly for global regulators looking at how these innovations may impact the operational resilience of financial sector within their remit. This includes not just the potential risk of new technology impacting the functioning of the financial sector, but also how technology may introduce security risks through the increased interconnectedness of services and providers.

[6] http://www.fsb.org/2018/07/fsb-publicly-consults-on-cyber-lexicon/

[7] Sample playbooks include those provided by CREST/National Cyber Security Centre (NCSC) ("Cyber Incident Response Scheme") and FS-ISAC ("The All-Hazards Crisis Response Coordination Playbook for US Financial Center"). While these have been developed with cyber security in mind, many principles can be extended to operational resilience in general.

Financial institutions have increasingly outsourced technology and information services to third party providers, as noted in section 1.5, many of whom may not be directly regulated. The introduction of innovative and/or disruptive fintech service providers has also increased the concerns around both cybersecurity and operational resilience, and FIA supports the concept of a shared understanding of minimum standards regarding operational resilience, as noted in section 1.10 of the Paper.

Another recent industry development has been the increased distribution of data away from clearly defined and understood nodes. For example, the transition from technologically heavy implementation of systems at individual financial institutions towards a centralised approach offered by cloud computing and other distributed information systems offered by third party providers is increasingly more common. The recent interest in distributed ledger technology as a more efficient approach to dissemination of information across various parties is also part of a trend towards dispersed information storage and services. Notable within the cleared derivatives industry has been the recent outsourcing of clearing at firms to utility service providers.[8]

Operational resilience of business services

Chapter 2 of the Paper explains why the supervisory authorities consider that managing operational resilience is most effectively addressed by focusing on *business services*. FIA supports this view since the trading and clearing of exchange traded and over-the-counter derivatives is typically performed within a business unit of a large global financial institution. Such a business unit may be relatively small in comparison to other business units within the firm yet provides a critical business service by supporting clients' ability to transfer risk to FMIs for cleared derivatives.

Although firms typically do not currently define their *business services* for the purposes of operational resilience, it is reasonable to expect them to be an extension of their resilience models, and to focus on business continuity rather than disaster recovery. We recommend that the supervisory authorities engage with firms to understand how they view business continuity across individual business lines.

An emphasis on business services will require a detailed mapping of end-to-end processes, applications and people, and will require significant effort to develop and maintain such a mapping. However, once the business services that are in-scope have been agreed, we believe that it is feasible to establish impact tolerances that are both meaningful and measurable.

FIA believes that such an exercise is valid where it has not already been undertaken, and that firms should look at their business services in terms of what they provide to the wider financial sector or economy in general, not just to the firm itself. For example, the clearing business of a large global financial institution may be relatively small within the firm itself but play a critical part within the cleared derivatives industry and the resilience of an FMI such as a clearinghouse. As such the firm should prioritise the resilience of this business service accordingly.

[8] https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/oct/Post-Trade-Investment-Banking-Outsourcing.pdf

Interaction of regimes and the need for cross-border coordination

As technology has increasingly enabled global market access, so the adoption of distributed and dispersed technology has also increasingly made financial institutions' operations global in nature, as noted in section 1.9 and chapter 2 of the Paper.

Firms may provide business services that span multiple international regulatory regimes. On page 21, the Paper notes that several large financial institutions are subject to the PRA's operational continuity in resolution (OCIR) policy, but they are also likely to fall in scope of the European Banking Authority's (EBA) Group Resolution Plan requirements under rules such as CRR or CRD IV. These firms are also likely to provide business services that are subject to the FCA's oversight under regulations such as the European Market Infrastructure Regulation on derivatives, central counterparties and trade repositories (EMIR), which also looks to minimise operational risk for firms and FMIs providing clearing services.

Cross-border and inter-regulatory cooperation is key to ensuring that global institutions focus on operational resilience itself rather than ensuring compliance with requirements under different regimes; requirements should be complimentary and not introduce contradictions that may require the creation of regulatory firewalls internally within a firm. In our view, unilaterally implemented regulation may disrupt the consistent implementation of business services internationally.

As we noted earlier, technology and operations are increasingly outsourced to third party providers who are usually not directly regulated. As such, financial institutions face their own challenges with regards to how they comply with different regulations regarding fintech, cybersecurity and operational resilience globally.

We have observed an increased regulatory focus on outsourcing services within several jurisdictions and would urge the UK supervisory authorities to adopt flexibility in their expectations around both intra-firm and third-party outsourcing. Firms' outsourcing models are linked to global operating models, and analysis has typically been performed between the outcomes delivered by onsite versus outsourced functions. Where outsourcing to a third-party provider has been deemed appropriate, oversight of the operational resilience of the providers is maintained and considered through assessments of the overall resilience of the firm.

As the Paper introduces some new concepts, we encourage the UK supervisory authorities to ensure that proposed requirements do not conflict with international approaches, including other existing regulatory initiatives such as the FSB cyber lexicon (already cited), the European Central Bank's Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU),[9] and the Basel Committee on Banking Supervision's operational resilience working group, highlighted as a priority in January 2018.[10]

Impact tolerances

The Paper introduces the concept of *impact tolerances* in multiple places, with chapter 5 discussing how impact tolerances may provide clear metrics for when an operational disruption represents a threat to a firm's or FMI's viability, to consumers or market participants, or ultimately to financial services.

[9] https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html

[10] https://www.bis.org/speeches/sp180129.htm

Whilst FIA agrees conceptually with the principles set out in the Paper, we have several concerns that we would like the UK supervisory authorities to review with industry participants further before setting expectations for the cleared derivatives industry.

Firstly, firms will need more detail on how authorities intend to use impact tolerances to assess impact and value, especially how they will relate to any future stress-testing (as well as how they may factor into stress-tests required under other regulatory requirements). While the UK supervisory authorities set out their expectations to allow firms to determine their own impact tolerances under a risk-based approach, the need to satisfy a stress-test on a pass/fail basis could necessitate firms adopting a "one-size-fits-all" approach that prioritises navigating the stress-test but fails to capture the resilience implications of firms' individual business models.

Secondly, firms will also need to be very clear on what defines a "vital" service and how a firm's contribution to it is measured to determine impact tolerances, and whether certain metrics are appropriate for different kinds of outages. It may not be appropriate to measure all impact tolerances in terms of time, for example a cyber-attack where, depending on the incident, the degree of impact could be very severe.

Thirdly, the Paper discusses board and senior management setting priorities for their own impact tolerances. This a point where we believe that proportionality is important. A large global firm that provides multiple business services will need to adopt a different approach from a firm that focuses on a particular business service solely within the UK financial sector; as such the global firm will require a broader principles-based approach in accordance with multiple regulatory requirements as well as those outlined in the Paper.

Finally, the Paper indicates that the Financial Policy Committee is considering also establishing its own impact tolerances for periods of disruption that firms will be required to meet, but gives no detail as to timing when this will occur, whether the process will be fully transparent, whether numerous firms will be subject to the same impact tolerances etc. It is important that firms are given clear expectations, which are made in collaboration and on a risk-weighted basis.

Supervisory assessment of operational resilience

Chapter 6 outlines four broad areas that a future supervisory approach could cover, notably sector-wide work including potential stress-testing, supervisory assessment of how firms and FMIs set impact tolerances, analysis of systems and processes that support business services, and assurance that firms and FMIs are compliance with existing rules, principles, expectations and guidance.

Firms' and FMI's adoption of recognised frameworks such as those produced by CPMI-IOSCO, FSB, NIST and NCSC, amongst others, are important to assessing how firms and FMIs have approached their operational resilience. Firms may choose to adopt a hybrid approach according to their own requirements, and therefore any supervisory assessment should be flexible enough to recognise differences in approach from any specific framework that may be used by the UK supervisory authorities to measure a firm's compliance; instead the supervisory focus should be through a due-diligence based review of the policies and procedures implemented by the firm or FMI.

To this point, FIA supports a principles-based approach to supervision which should assess the size of the firm or FMI, of its business services, and its scope within the UK financial sector, as well as its operational

resilience requirements within its home jurisdiction. This will allow the UK supervisory authorities to take a proportional approach for firms and FMIs rather than applying a one-size-fits-all approach to supervision.

Summary

In conclusion, FIA supports the key objectives of the Discussion Paper to promote business continuity and to maintain confidence within the financial sector in the event of a disruption to services.

For the cleared derivatives industry to continue functioning in the event of a serious disruption regardless of the type of threat, preparedness, recovery, communication and governance are key to maintaining confidence for industry participants, regulators and other industry observers. The approach outlined in the Paper regarding prioritising business services within firms is important to ensuring that ecosystems such as the cleared derivatives industry remain operational in the event of a disruption that impact multiple institutions. It is important that the clearing business within a firm is also operational to ensure that an FMI such as a derivatives clearinghouse continues to function as mechanism for mutualising risk across industry participants. As such, while firms should be able to prioritise their own business services within an operational resilience plan, there should also be an objective element regarding the importance of the service across the broader industry (for example as a "Critical Economic Function") rather than a subjective evaluation of its importance within a firm.

Many firms and FMIs are global in nature and provide business services within the UK financial sector. FIA recommends that UK supervisory authorities should follow a principles-based approach to supervising global firms' operational resilience that focuses on proportionality and assessing the appropriate level of due diligence within a firm's operational resilience program, encouraging firms to focus on the practices around resilience rather than compliance. We are encouraged by the approach taken in the Paper that recognises these points and expects further dialogue with the private sector to best meet the objectives of the UK supervisory authorities.

Respectfully submitted,

Greg Wood

Senior Vice President, Global Industry Operations & Technology

Responses to selected questions asked within the Paper

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?

FIA believes that it makes sense to focus on critical services or products - for example the role of FMIs and clearing members within the cleared derivatives industry. However, given the variation in terminology between the Paper and other industry frameworks, firms should have continued engagement with the UK supervisory authorities to further understand their expectations, allowing firms to make informed comparisons between the approach in the Paper and current practice - for example how will existing concepts like Key Risk Indicators, Key Control Indicators and Key Performance indicators work with the principles outlined in the Paper?

- A focus on business services will require detailed mapping of end-to-end processes, applications and people that will require significant effort to develop and maintain. Firms typically look at KRIs, KCIs and KPIs based on operational areas or key systems within the firm rather than using the concept of business services. Firms' difficulty in adapting will depend in part how the two approaches reconcile with each other.
- There is a risk that reconciling different approaches to resilience may introduce its own disruptions to a firm, and the scale of risk will depend on how the UK supervisory authorities define or view "vital" services, how broad the final scope is, and the number of firm's services that are included within that scope.
- As indicated in the Paper, there will be adjacent processes or services that require resilience as well - for example payments or reporting. These adjacent processes should also be prioritised when assessing key business services. However, we urge the authorities to retain a balanced approach in their expectations since firms will need to manage a complex environment of services and systems which may include many different stakeholders internal and external to the firm.

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?

- Business services that support critical functions within the financial sector and the broader economy are typically already recognised as high priorities in firms' resilience strategies, as per previous guidance from both the PRA and EBA on Critical Economic Functions (CEFs). OCIR lays the foundation for coverage of broader resilience scenarios. For most prudential firms this is largely based on the PRAs Recovery Plan (already cited) and on their Group Resolution Plan and Recovery Plan[11] under the interactive single rulebook provide by the EBA under multiples rules, notably CRR, CRD IV and BRRD, and we encourage the UK supervisory authorities to consider and additional requirements carefully to avoid duplication or conflict, if not already done.
- Again, firms would need to be very clear on what defines a "vital" service, how a firm's contribution to it is measured, and the extent to which firms could leverage existing work they have implemented as part of their Risk and Control Self Assessments (RCSAs). Without fully understanding how the requirements map to existing practice it is difficult to estimate additional costs to firms.

[11] https://www.eba.europa.eu/documents/10180/950548/EBA+Report+-+CFs+and+CBLs+benchmarking.pdf

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

- While operational resilience is a board-driven initiative, it is typical that the implementation is delegated to specific functions or roles within a firm, notably the Chief Operating Officer, Chief Information Security Officer, etc., with several further levels of delegation within the firm's business units to ensure that each unit meets the objectives of the firm's board and senior management.
- While we believe it is important for the board and senior management to instil a culture of operational resilience within the firm, it is ultimately more important for the UK supervisory authorities to focus on the framework used within the firm, and how processes and procedures are then implemented by senior management responsible for running the business units and supporting the operational environment of both their business units and the firm in general.

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?

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

- It is our view that once a mapping of applications/processes to business services and/or vital services has been completed, it should theoretically be possible to re-purpose existing metrics/reporting documents to meet regulatory expectations, including generating impact tolerances for relevant services. However, as we have noted in a previous answer, such a mapping requires further guidance from the UK supervisory authorities and may cause conflicts with existing operational resilience and/or risk analysis frameworks within the firm.
- Firms need to understand more about the UK supervisory authorities' views on how impact tolerances would be implemented for them to assess both effect and value to the firm, as well as the extent to which they can be compared to risk appetite statements that have been developed over recent years through frameworks such as RCSA.
- As we have noted, using a different approach to impact tolerances based on business services may demand a change in approach, necessitating more complicated cooperation between operational resilience and business units – especially where firms may have set tolerance levels based on service level agreements (SLAs) with their clients.
- While this is ultimately likely to improve resilience efforts, the implementation of tolerances must be pragmatic and recognise that real-life events may exceed what has been planned. Firms should try to respond within a reasonably judged impact tolerance but should not be negatively viewed if tolerances are breached – ultimately this is an iterative process that calibrates based on multiple events and responses.

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

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

- As we have discussed above, this would depend on the level of overlap or conflict between current practices and the proposed approach within the Paper, and we encourage the UK supervisory authorities to work with firms to provide further clarity on differences in approaches or terminology between the Paper and current practice.
- Concerns include:
    - The scope of business services and/or vital services, and the extent of overlap between these services and Critical Economic Functions (CEFs) as defined for resolution planning purposes, and already captured by our critical business processes mapping as per PRA and EBA requirements; and
    - The differences (or otherwise) between the metrics firms currently calculate in relation to "critical business processes" (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?

- As we have noted previously, once a mapping of applications and processes to business services and/or vital services has been completed, it may be possible to re-purpose existing metrics/reporting documents to meet regulatory expectations - including generating an impact tolerance statement. Again, it will only be possible to ascertain the difficulty in this task once we have more clarity from the UK supervisory authorities regarding their expectations for generating an impact tolerance and how far this overlaps or conflicts with existing practices, especially with regards to compliance with expectations across multiple regulatory jurisdictions.

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?

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

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

- In addition to our answers to previous questions, FIA wishes to highlight the following considerations:
    - We believe firms will require more detail on the different kinds of outages that will need to be considered under this proposed approach and would encourage the UK supervisory authorities to be flexible in their expectations. For example, impact tolerances for a certain business service will be different during a market-wide event compared to a firm-specific outage scenario and may be impacted by factors beyond one firm's control.

- We recognise the increased regulatory focus on outsourcing services across jurisdictions but would encourage regulators to look at frameworks that exist today for managing and overseeing third party and inter-affiliate service and support relationships. As we have noted, firms' outsourcing models are typically linked to global operating models with analysis between the outcomes delivered by onsite versus outsourced coverage of relevant functions. UK supervisory authorities' expectations should be pragmatic and based on understanding of what is achievable through a firm's oversight of third-party providers.
- It is important that the UK supervisory authorities do not introduce any requirements that would cause disruption to the operating model of global firms intended to provide significant efficiencies around providing clients with access to global financial services such as cleared derivatives market infrastructure. International consistency and harmonisation are key to global institutions taking a consistent approach to their global business services without creating internal regulatory firewalls to meet different jurisdictions' requirements.