UK Finance's response to DCMS Call for Views on cybersecurity in supply chains and managed service providers

1. About us

UK Finance is the collective voice for the banking and finance sector. Representing more than 250 firms, we act to enhance competitiveness, support customers, and facilitate innovation.

Executive Summary

On behalf of our members, we welcome the opportunity to comment on the DCMS's call for views. Prior to and since the publication of the call for views, we have engaged with members, providing them with opportunities to discuss the DCMS's expectations and sharing their individual responses on the questionnaire or otherwise.

UK Finance acknowledges this call for views as an opportunity for the DCMS to learn from the Financial Sector, considering how risk management related to supply chain and managed service providers must fit within existing programs for managing technology and cybersecurity risk. UK Finance through our response seeks to highlight the existing regulatory and compliance expectations placed on the sector and welcomes the opportunities to engage with DCMS on the actions of the regulatory bodies and the sector towards ensuring the resilience within our supply chain and managed service relationships.

We wish to highlight four areas, which we have discussed in more detail throughout our response.

1. Ensuring that the DCMS is aware of the significant activity underway in the financial sector, including several new regulations and guidelines, To provide legal certainty it is important any new policies or legislation are in alignment with existing sector-specific regulatory expectations. The policy outcome of the call for views should allow for flexibility especially for existing sector-specific benchmarks and standards.

2. There is a need to ensure that requirements are clearly understood for Managed Service Providers (MSPs) and expectations on both the sector and MSPs, (e.g. the ability to access resilience assurance information, speed of implementation) are defined with clarity. This is in order to avoid the potential for further conflicting standards and compliance issues.

3. This is an opportunity for the DCMS to bring the UK key infrastructure service provider (ISP) organisations and managed service providers together focused on addressing technology vulnerabilities. This ensures transparency in compliance to benchmarks and the expectations on MSP's and ISP''s to comply with regulatory requirements placed on firms by the government.

4. There is a need for the DCMS to call out cloud service providers (CSP) within its definition and expectations on MSPs especially as areas such as depth of reach, varying level of risk and resilience between CSP's and other MSPs.

1. Risk and Efficiency of Compliance

Regulators have emphasised the necessity for a robust governance and risk management framework. As such, across the banking sector, UK Finance's members maintain a rigorous Information & Cybersecurity Program designed to protect firms and their clients, support secure delivery of services, adjust to address the risks presented by an evolving threat landscape, and meet regulatory requirements, all while remaining technology agnostic and principal based.

These programs encompass the governance, policies, processes, assessments, controls, testing, and training efforts required by industry standards and regulators across the Financial Sector. Leveraging resources such as the Financial Services Sector Cybersecurity Profile (FSP)[1], risk and security policies and standards provide the foundation and establishes the administrative, technical, and physical safeguards for protecting our technology environment, facilities, and client information.

With the accelerating change in technology and an increasingly sophisticated cyber threat landscape, firms are expected to leverage their risk management framework to systemically and consistently identify, control, assess, measure, treat, and govern information and cybersecurity-related risks. This supports the management of existing and emerging risks in a manner consistent with the sector's risk appetite and tolerance.

Allowing for flexibility in the implementation of these frameworks ensure that firms at different stages of their resilience process continue to maintain and improve resilience without the pressure of unnecessary tight deadlines that can result in oversights and errors, as evident from recent enforcement action related to implementation of change management under aspirational deadlines. If new supply chain cybersecurity risk management programs or requirements are to be introduced, they run the risk of creating disjointed risk management processes that add burden on compliance teams, reducing overall resilience and effectiveness.

UK Finance acknowledges this call for views as an opportunity for the DCMS to learn from the Financial Sector, considering how risk management related to supply chain and managed service providers must fit within existing programs for managing technology and cybersecurity risk.

2. Conflicting Standards

Various regulators have developed and defined sets of requirements to manage the risks associated to supply chain cybersecurity, both internationally and in different sectors. Very few IT structures that achieve cybersecurity are 'jurisdiction specific' and therefore the regulatory position in multiple countries usually needs to be addressed. When you add the divergent approach taken by different jurisdictions in relation to data privacy (with data protection and personal data forming an important element of cybersecurity for many firms), the picture becomes further complicated. Although regulators share a similar goal of improving security, the proliferation of standards raises the risk of conflicting requirements and/or increases the cost of complying to multiple similar standards. The approach in the EU, UK, USA and other national settings does indeed contain similar aspects, but there are inevitable divergences creating concerns of conflicting standards that represent an

[1] Reference to CRI FSP page.

[2] FSB Discussion paper

[3] UK Treasury Selection Committee Inquiry on IT Failures in the FS Sector

[4] NIS 2 Directive

impossible task to comply with across borders. This poses a risk of the unintended consequence of creating disruption and subsequent regulatory intervention in response; for example, these issues have been raised by banks in their evidence to the UK Treasury Select Committee Inquiry on IT Failures in the FS Sector[3].

The issue of the different time scales for implementation creates further difficulties, resulting in the need for constant review and remediation. It is more straightforward for firms to develop a risk mitigation strategy for a single new piece of legislation that is being added to a body of pre-existing rules, than it is to formulate novel plans to deal with several sets of requirements that are each coming into existence at around (but not exactly) the same time.

Differences in definitions and terms in regulations can create problems considering the wide range of rules existing across multiple jurisdictions.

An example of the potential difficulties of different international requirements is evident from the area of operational resilience. Organisations are expected as part of their operational resilience requirements to identify critical business services and dependencies which includes their third party and outsourced service provider relationship. This discipline has seen broad agreement in approaches by the EU, UK, and US, but concerns persist regarding different standards, which are difficult to implement across borders. The new regulations in this area include:

- US regulators have recently announced final guidance on Sound Practices to Strengthen Operational Resilience
- The EU is expected to implement the Digital Operational Resilience Act as part of its cybersecurity strategy for 2021 and beyond; and
- The UK FCA and PRA will implement revised standards for outsourcing and operational resilience this year.

Taken together, the proliferation of guidelines and requirements represents a major compliance exercise for financial service firms. With the scope for both significant overlap and divergence between approaches developed at the national and international level and across various sub-sectors of financial services, it is essential that the UK Government consider the risk of conflicting requirements to respond to the quickly-changing landscape without placing excessive burdens on UK businesses that may in turn undermine the very aim of the regulations, namely achieving greater cybersecurity. Without international coordination and attempts to achieve alignment and consistency across sectors and regions, it will be difficult for business to maintain the highest standard of cybersecurity.

A particular issue the UK Government should consider is that pre-existing and new EU requirements that overlap with UK law implemented prior to Brexit. Relevantly, NIS was implemented in the UK prior to Brexit and NIS 2[4] is likely to be introduced across the EU in forthcoming years. As part of NIS 2, it is expected that companies subjected to the regulation will be asked to carry out assessments of the security of their supply chains and supplier relationships. Especially where they have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of their network and information systems by exploiting vulnerabilities affecting third party products and services. On the European level, information exchange will be strengthened and representatives of Member States, the Commission and ENISA, will carry out coordinated sectoral supply chain risk assessments with the aim of identifying per sector the critical ICT services, systems or products, relevant threats and vulnerabilities.

The Financial Stability Board's (FSB) Discussion Paper[2] on Outsourcing identifies areas of international convergence at the highest level in this area that can be drawn from the approaches of domestic regulators. In turn, the Paper recognises how regulators can work together to develop common standards that are maturing across geographic boundaries. For example, areas where there is international consensus on the steps to follow at a high-level are the need for institutions to implement a risk-based framework to address and prepare for outsourcing, to prepare and test business continuity and exit plans, and to use proportionality in implementing measures particularly in respect of intra-group arrangements and governance. Lessons can be drawn from the learnings in this paper.

3. Lack of transparency

The UK Government should consider ways in which it can help to provide the transparency businesses need to assess the risks. For example, challenges exist for financial institutions in relation to the management of risks associated with sub-contractors of any tier ("nth parties") which can affect the ability of firms to mitigate against those risks. From a due diligence perspective, some suppliers can be reluctant to disclose how they conduct due diligence of sub-contractors. Similarly, issues can arise as a result of some providers' views that cloud providers are not sub-contractors. There are also challenges with the ability to adjust pre-existing sub-contracting arrangements. Providers can therefore be reluctant to amend those existing contracts in line with new and additional requirements of financial institutions.

As to the exchange of information, the UK Government could provide support to businesses to facilitate the provision of information. The sharing of information via a supply chain register may allow the effective and collective identification of risks that will be impossible for businesses to identify individually. However, if such a register were to be introduced, government and regulators will need to take a lead role in providing the required framework and work towards an international register that does not place excessive disclosure requirements on businesses.

It is important to ensure that any oversight contemplated is consistent and interoperable globally with new and existing standards. To the extent that this is not the case, this will arguably exacerbate the risk of numerous regulators conducting fragmented supervision. This may present downstream risk to financial institutions where resources and capabilities are dedicated to this oversight as opposed to the continued provision of safe and secure services to financial institutions. The scope of any initiative to oversee cybersecurity is also important to consider in the context of the nature of the third party that is providing the service. It will be appropriate to consider the compliance requirements on third parties and to tailor the scope of any further guidelines or policies accordingly, whereby consideration is given to whether the risk that the regime seeks to address is already catered for as part of an existing regulatory or compliance requirement.

The Government should seek to provide clarity especially in the following areas:

Limitations on access, audit and information rights:

Limitations on access, audit and information rights can pose a challenge for firms, particularly where suppliers are reluctant or unwilling to provide appropriate access and/or re-negotiate contracts. These risks could also be addressed by facilitating the exchange of information and providing a mechanism to require disclosure of information by third party suppliers (see above).

Principle base regulation: Proportionality

UK Finance has supported an approach that allows for regulatory requirements to be applied on a proportionate basis, where firms are able to place reliance on their existing policies and processes to address certain supply chain requirements. As regulatory requirements for monitoring and managing third-party risk evolve and the regulatory environment becomes correspondingly more complicated, the necessity of looking to principles over prescribed rules increases. While we recognise authorities will remain focused on operations under their jurisdiction, we firmly believe that fragmentation to firms' global operating models, for example in the way they provision IT or control for cyber risks, will increase risk and reduce resilience counter to the policy objective of the regulations.

At the level of senior management of businesses, proportionality is also particularly important. Consistently with regulators' approach to outsourcing/operational resilience, generally, the UK's FCA's and PRA's SMC & R is designed to apply in a proportionate and flexible way to accommodate the different business models and governance structures of firms, which applies equally in respect of oversight of cybersecurity, as well as operational resilience and outsourcing.

Although principle and objective based regulation should be utilised to achieve resilience in outsourcing, there is widespread support for guidance on certain areas, albeit with concern that guidance is not overly prescriptive, inflexible, or rigid and exclusionary of alternative methodologies.

Concentration risk

There is the possibility of systemic risk arising from concentration in the provision of services to financial institutions. In this respect, it is important to differentiate between the concentration risk that may exist where a group is dependent on a single service provider for the provision of tasks, and instances where multiple regulated entities use a common service provider. In the case of internal dependency, firms should be able to undertake this as an internal assessment, based on risk appetite, and not be mandated to assess this on stipulated metrics that are set in regulatory guidance. On the other hand, in the context of multiple regulated entities using a common service provider, this presents a challenge for financial institutions who do not have oversight of the dependence of peer firms. The measures to address lack of transparency outlined above, could help to address the problem of concentration risk across multiple entities.

4. Managed Service Providers – Cloud Service Providers

UK Finance has observed that cloud service providers are considered Managed Service Providers (MSPs), as for the purposes of this Call for Views. However, we note that unlike *traditional MSPs* - as described in this paper - cloud providers do not have '*widespread and privileged access to the networks, infrastructure and data of their customers*'. Access to customer data and networks is in most cases limited and segregated, both legally and physically, which is regulated by the UK, EU and global privacy rules (in particular GDPR where cloud providers are processors of customer data and only access that data based on customer instructions - which is for technical support and maintenance purposes). Equally, the misconception that public cloud - by pure inclusion into the MSP category - poses '*disproportionate risks to the security and resilience of organisations across the UK*' as suggested in the initial consultation paper, needs to be re considered and clarity on the risk and resilience of cloud service provider called out.

It is also important to emphasise that the presence of cloud as part of a managed service arrangement should not act as an automatic indication of risk without an appropriate assessment. For example, a private cloud that is wholly owned and managed within a corporate group is much closer to traditional on-premises models of IT provision than some other uses of cloud. Under certain arrangements, the cloud infrastructure could be owned, operated and provisioned for exclusive use

by a single corporate group. As such, the firm's legal entities would have enhanced oversight of, and input into the design of, the mitigating controls put in place. As a result, such engagements (e.g. engagements that are supported by applications/systems that are hosted on a private cloud or data that is processed via a private cloud) should not be automatically perceived as more susceptible to risk than that provisioned through traditional hardware models. Given the benefits that can be obtained through the use of cloud, as recently noted by IOSCO,[2] where all cloud models are treated in the same way and subject to heighted regulation it may stifle the ability to realise these benefits, while not being commensurate with risk.

The Bank of England/PRA commissioned report, The Future of Finance, explains that the Bank should embrace cloud technologies, which have matured to the point they can meet the high expectations of regulators and financial services. It offers the advantages of business agility, faster innovation and cyber-defences to provide better services to households and businesses. It also enables large firms to take advantage of the skills and talent in small and medium-sized businesses. Notably, forty-three per cent of the UK financial sector said they thought complex regulatory requirements were the key barrier to adopting cloud collaboration according to a new Finastra survey (see Future of Finance Report at page 10 available here: The Bank's response to the Future of Finance report, see here shows that the Bank has acknowledged the importance of working with the private sector to help firms realise the benefits of public cloud usage without compromising resilience.

Finally, UK Finance acknowledges that assurance over cloud service providers within the financial sector, specifically the larger CSP's is problematic. Given the size and commercial power of these providers, this presents an opportunity for DCMS to consider assurance expectations in place within the Financial Sector or a commercial incentive to improve how assurance can be measured and provided.