DCMS Call for Views: Cyber Security in Supply Chains and Managed Service Providers

UK Finance response to DCMS Call for views on Cyber Security in Supply Chains and Managed Service Providers.

About us

UK Finance is the collective voice for the banking and finance sector. Representing more than 300 firms, we act to enhance competitiveness, support customers, and facilitate innovation.

On behalf of members, we welcome the opportunity to share our collective questionnaire response on the DCMS's call for views. Where possible, we have aimed to provide context as part of our response.

Part 1: Supply Chain Section

Questions on Barriers to Effective Supplier Risk Management

1. How much of a barrier do you think each of the following are to effective supplier cyber risk management?
    - Low recognition of supplier risk – Severe barrier. There is a need to ensure supplier minimum control requirements are defined and included in the contract. It is also existent where a pre assessment has not been conducted and where the suppliers end to end processes are not clear. Mis classification of risk is another barrier in addition to low recognition.
    - Limited visibility into supply chains – Somewhat of a barrier but can be severe if audit rights via supplier control assessments are not included in the contract. Depending on the services being provided, this can pose a major issue where the risk posed is through the relaxation in controls or a varied approach to security/cyber controls within the chain between 3rd and 4th parties.
    - Insufficient expertise to evaluate supplier cyber risk- Somewhat of a barrier but can be severe if supplier control assessments are performed by inexperienced technical SMEs. This is a fundamental risk as supplier risk evaluation is more than a tick box exercise, it demands that the reviewer understand where and how suppliers will be used.
    - Insufficient tools or assurance mechanisms to evaluate supplier cyber risk- Not a barrier as there is an abundance of various tools, methods, and hypothesis on how to conduct cyber assurance for suppliers. It becomes somewhat of a barrier when it is related to how they are applied and how the end to end processes including legal, procurement, security, work together to enable assurance at all levels.
    - Limitations to taking action due to structural imbalance- Not a barrier as security control requirements are embedded in contract language and supplier minimum controls. It can be somewhat of a barrier when there is a break in end to end processes as highlighted in the point above.

2. Are there any additional barriers preventing organisations from effectively managing supplier cyber risk that have not been captured above?

Response: Yes

3. [If Yes] What additional barriers preventing organisations from effectively managing their supplier risk are you aware of?
    a. Increase in regulatory scrutiny and inconsistencies in regulatory guidance.
    b. Continuous engagement with suppliers, huge task to evaluate supplier risk each time the risk landscape changes/ service changes, example cloud technology
    c. Contractual refresh may be required each time cyber risk profile changes. Banks cyber-risk appetite and what we deem to be suitable controls may change at a faster pace than what is feasible to update contracts
    d. Mutually agreeable T&C's that allow for red teaming. Mutual agreement for threat analysis and potential impacts. Integrated incident management and data sharing of incidents. Potential different levels of appetite/policy and control standard.
    e. Suppliers received multiple requests with sometimes vastly different expectations, when in their own mind, they are 'just' offering a solution. They struggle to cater for the masses' different requirements for the delivery of said solution(s). The smaller suppliers will be eager to cater for all and may break their own security model to do so, where the larger suppliers are less likely to accept any amendments and/or niche requests from costumers. Although the latter may not be less secure, it may require firms to risk accept gaps, where standing contractual templates or security controls can't be adhered to. This can in some cases pose an issue from two perspectives; (i) the risk profile within the firm will not reflect its aspired risk appetite and thus projects a misbalanced scorecard, or (ii) the threat landscape is wider than projected and potentially unknown.
    f. Legacy contracts, sometimes lack of co-operation by the third parties, assurance of the controls information provided in a response to a questionnaire by third party and lack of transparency by third party if there is an abrupt change to its cybersecurity profile after the validation or certification
    g. Large suppliers often will not even take part in such assessments. Organisations do not take the completion of these assessments seriously and do not always assign the correct staff to complete – this could be connected to the significant scale of requests they receive which generates an unmanageable compliance burden. The questions and time needed to undertake good quality assessments is considerable on both sides, this requires expertise to fully understand the third-party risks including cyber risks.
    h. Where supply chain risk assessment is conducted it is often point in time and effectiveness can be influenced by the experience of reviewer, time available and quality of information provided during reviews. Paper-based reviews and adherence to control frameworks are not measures of effective security, and while compliance to a framework may show good intent it may offer a false sense of security.
    i. Lack of understanding of the criticality of the supplier to the business is a root cause of other failings in the supply chain.
    j. There is often a reliance on the contractual basis of the supplier at the loss of actual assessment of the supply chain risk. Reputational impact isn't limited by contracts that make suppliers liable, therefore the contract provides limited real-world protection. On the whole breaches of significance are unlikely to be as a result of a control dictated by a contract failing, this can potentially lead to a cycle of constantly updating the contracts to the latest position.
    k. There is also a need to understand not only the supplier from an organisational perspective but the services the supplier provides and the associated risk each service may pose to the resilience & security of the client.

Questions on Supply Chain Cyber Risk Management

4. Have you used the NCSC's Supply Chain Security Guidance?

Response: UK Finance observed most of the smaller organisations said yes while most of the larger ones said their current supplier due diligence, oversight and continuous processes align with NCSC security guidance. A smaller number said No.

5. How challenging do (or would) organisations find it to effectively act on these principles of supply chain cyber risk management, as outlined in the NCSC's Supply Chain Security Guidance?
   - Understanding the risks – Not at all challenging as most organisations tend to ensure their procurement process includes the understanding of risk, this is often driven by cost and has at late incorporated information/cyber security. It can be hard to get great clarity on risk if the supplier is not willing to be vulnerable and share details. Suppliers may understandably view disclosure of known vulnerabilities to a broad number of their customers as a risk.
   - Establishing control – Slightly challenging as control within the e2e procurement and supplier management process is often difficult if security teams are not part of the RFX process form the start and furthermore not included in the ongoing supplier management process. Key point at late has been that monitoring needs also, to extend to connecting operational response time with security monitoring. Otherwise, not at all challenging.
   - Checking arrangements – On average, slightly challenging. Checking arrangements is key to successfully managing a supplier relationship. KPI's is something some organisations may be challenged with. In particular the smaller organisations that do not have the skills and resources to manage the oversight and monitoring of a supplier.
   - Continuing to improve, evolve and maintain security – This varies between slightly challenging and very challenging. Here we come back to the risk that suppliers may be unlikely to want to cater for niche requests, if not baked in at the start (through procurement or contractual obligations), unless an incident has occurred.

6. What are examples of good practice for organisations implementing these aspects of supply chain cyber risk management?
   - Open question

   a) Understanding the risks
      a. identification of key risk attributes, inherent risk calculation, understanding overall criticality of supplier to the organisation based on a consistent methodology, knowledge of services provided and the risk appetite of the business. This allows the inherent risk position of the supplier to be known and a segmentation based on the risk profile to be categorised i.e. most critical to low. To assess the risk to an organisation it must first understand its threats and potential areas of vulnerability. Using a consistent methodology such as STRIDE a scorecard of the supplier can be created highlighting the risk posed by the supplier.
      b. Supplier risk assessment, continuous updates/ engagement as the service/ risk landscape changes
      c. Supplier assessment Due-diligence – in depth review of supplier and cyber controls pre-contract
      d. Understanding of data that is held/exchanged between 3rd parties. Standardised and consistent data gathering is key to drive governance.
      e. Adopting a risk-based approach so the greatest rigour is applied to the suppliers that present highest levels of risk
      f. To have references such as Risk appetite, RCSA to contextualise and drive priority.
      g. Clear visibility and governance covering all stages of the supplier lifecycle. Mature criteria to identify and treat associated cyber risks within the supply chain without limiting it to third parties.

b) Establishing control
    a. Having established the risk profile of the supplier and the threats relating to the service organisations should be identifying relevant controls to improve their posture this may utilise industry standards (NIST, NCSC etc). The evaluation of the relevant threats, the minimum standards expected of the third party can then be specified and should also closely correlate to the internal controls / policies.
    b. The contract should then contain a suitable Security Schedule which details those minimum standards the organisation deems critical.
    c. Where organisations dictate the use of their T&C's these should align to NIST / NCSC or other external industry standards and be aligned back to the minimum standards / security schedule of the acquiring organisation. Allowing flexibility is important in this regard.
    d. Making suppliers aware of their obligations, having the obligations readily available via the internet, communicating when these are refreshed
    e. Communication of minimum control requirements to suppliers, assessment framework based on these control requirements, and control effectiveness scoring. Building security requirements into contracts.
    f. Ensure service provision and contracts are reviewed by stakeholders with security expertise, as well as commercial, legal, credit, financial crime
    g. Run campaigns/ training on specific cyber risks
    h. On-site/remote assurance activity on an annual basis
    i. In-house SMEs providing guidance on security control requirements
    j. Comprehensive internal supplier database containing relationship owners, service, and network connectivity topography, provided services, data ownership
c) Checking arrangements.
    a. Review recent penetration tests performed on high-risk suppliers or commission one, use AI tooling to scan high risk suppliers' cyber footprints on a regular basis and communicate deficiencies to them, ensure breach reporting and management arrangements are robust, perform joint readiness exercises if possible
    b. This and the proceeding question should involve cyclic processes reviewing threats and checking for vulnerabilities and asset changes to see if new issues emerge that may lead to intolerable risk. This includes on-site/remote assurance activity on an annual basis, or when the threat changes e.g. zero day/SolarWinds as part of your continuous monitoring program.
    c. Throughout the supplier lifecycle the treatment standards for the suppliers from onboarding through to exit processes should be aligned to the inherent risk profile of the supplier. For the most critical suppliers this should include such elements as annual onsite due diligence, reviewing independent attestations, regular "Keep in Touch" calls through security SMEs to security SMEs, and finally the rigorous assessment of any remediation activities to confirm gaps have been closed effectively. For the low risk suppliers this could be relying on self-attestation
    d. As part of your pre-arrangement checks the following examples are done as good practice:
        • Use of a questionnaire followed-up with an Interview.
        • Seeking evidence in the form of policy or evidence of execution where possible.
        • Understand their Operational Risk Governance, reporting line, escalation and how 1/2/3LOD operate in the company.
        • What is held in the cloud

d) Continuing to improve, evolve and maintain security
    a. On-going Service review/ security reviews
    b. The organisation should undertake an annual review of such artefacts as the minimum standards and assurance question sets, updates to security schedule,

renewals / extensions of contracts include latest version of security schedule to ensure that they reflect the latest updates.

c. Agreed set of key controls & performance and risk metrics, that are refreshed regularly.
d. Risk-based approach for supplier control assessment frequency (i.e. annual basis for high risk suppliers)
e. Maintain regular dialogue with critical suppliers, obtain information security metrics and information security assurance on a regular basis, understand their technology and cybersecurity roadmap
f. For most critical suppliers setting up a partnership type relationship aimed at sharing threat intelligence
g. Conduct analysis of incidents and emerging threats helps evolve and maintain security.
h. Continual assurance of key suppliers to check for vulnerabilities and asset changes to see if new issues emerge. Sharing intelligence across organisations / government. There is a network of business resilience centres throughout the UK for example Scottish Business Resilience Centre, primarily funded through a home office programme with a small annual subscription by its members. The intention is that organisations have the skills and knowledge to protect themselves against online attacks through education and such support as "Exercise in a box", Minimum standards utilising the NCSC guidance & questions. There is also the Financial Sector Cyber Collaboration Center (FSCCC) focused on sector wide incidence response and threat monitoring, co-sponsored by UK Finance and Bank of England.

7. What additional principles or advice should be included when considering supply chain cyber risk management?
   - Concentration, resiliency of supplier, Plan B, classification of service & volume of usage for the service.
   - Risk-based approach for supply chain cyber risk mgmt. scope (i.e. low risk suppliers have less due diligence)
   - Low risk suppliers should not necessarily be held to the same security requirements / oversight compared to higher risk suppliers based on service being provided or data sharing involved.
   - The firm/customer is liable and responsible for the risks posed to the firms' systems, data, and customers/consumers. Risks will not be delegated or transferred, even in a shared model. Approach the 'problem' with this principle in mind.
   - Ensure supply chain cyber risk management is integrated into the global/organisational supplier risk management.
   - Focus on the 'run' part of any arrangement. Often the focus is heavily on the on-boarding of a supplier and assessing cyber risks during the on-boarding. This focus should continue when the arrangement is operational or in 'run' state.
   - It should be a layered approach and include such factors as portability, geography (i.e. where the data is hosted), exit strategies and a platform for data / intelligence sharing. As described above the risk assessment must come first and then the extent and rigour of the other aspects, controls and oversight should be proportionate to the risk.

Questions on Supplier Assurance:

8. Have you used or do you plan to use the NCSC's Supplier Assurance Questions?

   Response: Yes, the majority of UK Finance members either use or plan to use the NCSC's supplier assurance questions. Others mention that the Supplier control assessment questions aligns to risk framework which covers NCSC assessment questions, while a small number use supplier assessments and scorecards based on ISO27001 and FS industry regulation, ENISA

and CSA cloud guidance are also reference points in addition to performing GDPR privacy impact analysis. Members indicate they value highly the ability to choose between different frameworks and do not believe any one framework or questionnaire should be made mandatory.

9. Since publishing the NCSC's Supplier Assurance Questions, it has been noted that the guidance could also cover the use of supplier-provided apps (e.g. where a supplier requires use of apps on an organisation's network to deliver its service to that organisation). Are there any additional areas of supplier assurance that should be outlined?

   Response: N/A

10. [If Yes] What additional areas of supplier assurance should be outlined?
    - Members indicate that while other areas could be covered, this should only be done at the level of guidelines rather than regulatory or legislative requirements.
    - Information classification and labelling
    - Asset management
    - Vulnerability management
    - Training
    - Disposal of assets
    - Cloud security
    - Cryptography
    - Endpoint security
    - Remote Access
    - Data leakage prevention
    - Logical access management
    - Control expectations for supplier's subcontracted services (i.e. Nth Parties). Though the PRA's supervisory statement (SS2/21) mentions fourth/supply chain however,
    - The firm/customer is liable and responsible for the risks posed to the firms' systems, data, and customers/consumers. Risks will not be delegated or transferred, even in a shared model. Approach the 'problem' with this principle in mind.
    - Guidance on when penetration testing should be used
    - Operational Resilience, Software Development Life Cycle (SDLC), Security Testing frameworks

Questions on Commercial Offerings:

11. How effective are the following commercial offerings for managing a supplier's cyber risk?
    Response: Further work needs to be done here to obtain clarity on risk and resilience requirements. More details below.
    - Private supplier assurance - On average, this is somewhat effective as private assessment companies are used successfully today to conduct supplier control assessments on behalf of the firm..
    - Platforms for supporting supplier risk – This is not effective as these platforms are not leveraged today and so there is no way to ascertain benefit or effectiveness. The Financial Sector is in the process of developing a standardised supplier risk management methodology underpinned by the Bank of England's Operational Resilience Standard and this will be aimed at providing a platform for supporting supplier risk.
    - Supply chain management system providers – This is same as above with procure-to-pay on organisations future roadmap.
    - Risk, supply chain and management consultancies – Same as above, somewhat effective on average.
    - Suppliers of outsourced procurement services – Same as above with responses ranging between not effective and somewhat effective.

- Industry cyber security certification schemes – This is somewhat effective with this presenting an avenue for additional data point and benefit to supplement supplier assessment.

12. What additional commercial offerings, not listed above, are effective in supporting organisations with supplier risk management?
    - Each of these offering is limited in isolation, but in aggregate these offerings, aligned to the right framework, should form the basis of an effective supply chain security assurance regime. Consideration of a Security Rating service may also be effective.
    - Potentially providers of tokenization solutions, which does not fit the description provided for (b).
    - Embedding NIST maturity level (commercially). An independent, on-site testing which is able to be commercially available – this may be covered in "Private Supplier assurance", however the information sharing is key.

Question on Additional Government Support:

13. How effective would the following government actions be in supporting and incentivising organisations to manage supply chain cyber risk?

    - Awareness raising of the importance of supply chain cyber risk management through the use of campaigns and industry engagement – This is somewhat effective though additional awareness would be beneficial. For medium to small organisations, this will be very helpful, however, larger firms typically already use these to furnish their existing procedures and methods. There may be more the NCSC can do to promote these to less-mature sectors.

    a) Additional support to help organisations to know what to do, such as:
        - Improved or additional advice and guidance
        - A tool that draws on existing advice and standards to help organisations manage supplier cyber risk

        Response: This is recently very effective with a caveat that additional guidance and direction would be beneficial in standardisation with the need for more focus on improvement and advice aimed at the suppliers. It is critical for firms/organisations to recognise and manage risk, but equally, it is key that suppliers themselves get better at their own security.

    b) Providing a specific supplier risk management standard that:
        - Outlines minimum and good practice and/ or
        - Provides assurance that an organisation is managing their supply chain cyber risk

        Response: Same as above. Setting minimum expectations that allow for flexibility across the sectors with existing compliance requirements and provide a baseline is welcome.

    c) Targeted funding to help stimulate innovation and grow commercial offerings that support organisations with their supplier risk management (e.g. Government competitions, accelerator programmes)
    Response: There are a number of good initiatives that aim to do similar. On average, this will be somewhat effective provided the government seeks to align/partake/support as opposed to reinvent.

    d) Regulation to make procuring organisations more responsible for their supplier risk management.

Response: Additional regulations could add unnecessary burden and would not be effective. The key to success here is to make the support proportionate (size of firm, size of supplier, size of risk) and even better, to make suppliers responsible for the security of their own products, processes and resources of which they supply to firms/organisations. This is where the effectives of a regulation from the government would be felt.

e) Other (Please specify)

- Reiterating the need for harmonisation and consistency in regulations in terms of definitions and scope in managing supply chain cyber risk as highlighted throughout this section.
- Where there is a concentration of use of critical parts of the supply chain and a potential aggregation of risk due to shared use there is a possibility to leverage a 'utility model' of assessment. This approach would mean alike acquiring organisations could share some reporting to reduce the impact on the supplier and overall costs by consuming one single shared assessment report independently undertaken by an external assessment organisation. This can then be included in multiple acquiring organisations wider supplier assessment frameworks. The Financial Sector has been successful in piloting this shared utility model and this present an opportunity to learn lessons from the ongoing work in this space.

Part 2: Managed Service Provider Section

14. What additional benefits, vulnerabilities or cyber risks associated with Managed Service Providers would you outline?

Response:

- Both customer and service provider security controls must be defined.
- Setting security requirements for both customers and providers are essential since reliance is on both parties.
- Possibility of competing priorities and sometimes confusion or misunderstanding of risk ownership.
- Managed service providers to fill gaps in capability, and to take control of commodity tasks that can be easily handled. The benefit of this approach is huge – users can tap into expert resource of great depth, and it frees the colleagues to specialise.
- Businesses should be aware of the significance and their responsibility for the security of client configurations. If MSPs use proprietary data formats that creates vendor lock-in.
- Certain MSPs may provide a better service to customers than can be offered internally and can improve control such as resilience options.
- Whilst it is true that controls at MSPs may vary, it is also true that recipients can control the minimum standard of control through effective risk identification, contracting, due diligence and ongoing assurance.
- Systematic risk and concentration risk across the industry is a real problem that cannot be solved through individual banks managing their own risk.
- Total outsourcing of critical services such as Network, Infrastructure or Security Operations Centres as Managed Services adds to the benefits such as: access to skilled resources, enhance the maturity of the processes but also could expose the organisation and create significant impact if cyber risks that are not identified and treated appropriately by the provider materialise.
- The greater risk is not at the MSP but at the organisations who fail to understand their outsourcing and incorrectly validate suppliers control positions. The bigger challenges are around nth party suppliers and the aggregation of risk that is unseen with underlying supporting parties

- Those providing infrastructure and connectivity are essentially part of critical national infrastructure by virtue of the service they ultimately support. For example, BT where there will be a definite concentration of use across industries.

15. Are there certain services or types of Managed Service Providers that are more critical or present greater risks to the UK's security and resilience?
    - Critical utilities such as Telecoms and other utility providers.
    - Niche ones where capabilities are scarce.
    - .
    - MSPs who handle or process large volumes of personally identifiable information are likely to pose a greater risk.
    - Cloud providers may become systemic to the functioning of the wider economy. However, given their geographic footprint, an international approach should be prioritised.

    In summary, UK Finance members note that there has been significant attention on this area in recent financial services regulation. Any intervention from DCMS should take into account sector specific activity and regulations and ensure interoperability and flexibility so that firms are able to prioritise risk management over compliance activities. .

16. When considering the 14 Cyber Assessment Framework Principles, how applicable is each Principle to the cyber security and resilience considerations associated with Managed Service Providers? Please choose one of the following for each of the 14 Principles

    Response: Overall the Cyber Assessment Framework Principles are high-level and standard supplier control expectations. Most organisations within FS cover most if not all of these principles in existing supplier control requirements, assessments, and due diligence oversight. Therefore, we acknowledge these as all completely applicable.
        - Governance
        - Risk Management
        - Asset Management
        - Service protection and policies process
        - Identity and access management
        - Data security
        - System security
        - Resilient Networks and systems
        - Staff awareness and training
        - Security Monitoring
        - Proactive security event discovery
        - Response and recovery planning
        - Lessons learnt

17. Can you identify other objectives or principles that should be incorporated into a future Managed Service Provider security framework?

Response: In general, there isn't much difference in how you manage information security/cyber for managed services providers, from the inside out. It becomes more important to understand the inside of the organisation, on top of already good third-party practices.

Some other key principles include:

- Information classification and protection
- Secure data destruction upon termination, deletion/destruction of physical and logical information.
- Definition of roles and responsibilities, service levels and agreements.

- Include cybersecurity objective and principles for the 4th party, offshoring by 3rd party and usage of Cloud including cloud computing.
- Cyber threat of the supplier as single point of entry to be used as a wider attack.
- The principles are fairly comprehensive and broadly aligned with other industry good practice
- Remote access
- Endpoint Security
- Threat Simulation/ Penetration Testing/ IT Security Assessment
- Cryptography
- On-site testing

18. How effective would each of these options be in promoting uptake of a future framework for Managed Service Provider cyber security and resilience?

Response: The key for all of these is to ensure that there are no further complications introduced to the definitions of managing third parties, but to identify opportunities for shared procedures, best practices etc. Where there is a niche distinction however, relating to the management of MSP's and services offered, there may be a requirement to call those out specifically.

- Developing education and awareness campaigns – Very effective but additional awareness is always welcome.
- Establishing a certification or assurance mark – Very effective as this could be used as a supplement to supplier control assessment.
- Setting minimum requirements in public procurement - Setting baseline requirements is considered essential and therefore will be very effective.
- Developing new or updated legislation – Somewhat effective. This would ensure compliance and enforcement but the goal towards ensure its effectiveness is aligning to existing compliance requirements and where necessary, updating said requirements.
- Creating a set of targeted regulatory guidance to support critical national infrastructure sector regulators – Somewhat effective but as the above point states, the government should consider alignment and flexibility in setting further guidance to support the critical national infrastructure where the Financial Sector makes up a key part of the CNI.
- Developing joined-up approaches internationally to managing Managed Service Provider security issues - Very effective as it will ensure consistency in compliance across the Managed Service Provider universe.

19. Please explain why you have provided the responses above and whether there are alternative ways the government could help address the cyber risks associated with Managed Service Providers?
    - Regarding (a) developing education and awareness campaigns, UK Finance members have answered 'very effective' because it is important for customers of these services to understand they retain accountability for the security of their data, whether it is processed in-house or, on an ever increasing basis, by MSPs. Furthermore, the more the wider collective population understand and expect good security practices, MSPs will have to operate at the highest levels or face getting left behind by their competitors, and ideally effective security should be built-in to services provided and not just be for those that can afford it.
    - We also consider (b) establishing a certification or assurance mark to be potentially 'very effective'. Rather than many businesses each asking similar questions and MSPs answering them many times over, customers can take a degree of comfort from a security certification. In reality, the larger MSPs usually only provide generic pre-prepared responses for info-sec assurance requests. This has the potential to effectively democratise security assurance because in bigger firms, it may assist in through-lifecycle management

by contract owners in business units, as opposed to being the preserve of specialist technical functions, and in small businesses who lack the skills and experience it makes such assurance viable. Larger firms, and those that operate in regulated sectors would likely use this as one element of their overall supplier assurance strategy, but it would be useful.

We would raise some caveats however. To be truly effective this should be independently verified (not self-certified), and those bodies that perform the verification should be monitored themselves that they are discharging their responsibilities thoroughly. Furthermore, there should be the right balance between principles based and prescriptive expectations so that it does not become a tick-box exercise, and the syllabus should be reviewed on a continuous basis as the threat landscape evolves.

- For (c), setting minimum standards in public procurement is less relevant as most organisations in FS do not operate in that sector, however we understand that public sector bodies stipulate suppliers must meet certain criteria to be eligible to provide IT services so something to strengthen what is already there could be useful for the sector.
- We consider (d) Developing new or updated legislation to be somewhat effective, this is from our perspective of already operating to regulatory requirements around data security and supplier management. UK Finance members are in the Banking and Finance entities and therefore operate in a highly regulated sector. We are certified against ISO27001, PCI-DSS and other standards, and adhere to NIST Cybersecurity and other such frameworks. There are high levels of expectations from our Regulators around the topics discussed in this survey, notably around Operational Resilience (which includes suppliers and information security as central pillars), the EBA Guidelines on ICT and Security Risk Management, and EBA Guidelines on Outsourcing, and recently the PRA's Supervisory Statement on Outsourcing and third party risk management. We have dedicated resources across the three lines of defence in respect of how the associated risks are managed and we are continuing to mature and refine our approaches.
- We consider (e) to also be somewhat effective for the reasons given for (d).
- We were not able to effectively answer (f) and have replied ‘don’t know’ because UK Finance is engaging presently with the regulators and cloud service providers communities respectively on the current developments on Schrems II and the movement of data between countries with legislation under development, particularly for a post-Brexit UK.

Other responses:

- All of the above would provide a consistent approach to cyber security requirements which should, alongside training, ensure cyber security risks are understood and correct mitigating controls implemented to reduce the risk. It would also reduce time spent on new engagements with service providers where minimum requirements/best practises are already designed and operating effectively.
- The development of a joint international approach may serve difficult and conflicting in the long run. An option would be a public – private partnership through already well-established groups; G7, IOSCO etc. The suggestion would be to research the feasibility of this with recommended groups, prior to engaging in the decision to form something. We see regulatory guidance and oversight as critical factors in improving MSPs’ security posture. Certification schemes will provide benefit but are strengthened by delivery in the context of a legislative or regulatory framework.
- Regulator may consider updating its Company House registration process whereby it includes a question if the non-financial company is providing IT support/service to a regulation company.
- International coordination is always challenging due to different priorities and maturity of the regulators in respective jurisdiction.
- Certification could be very effective if it can be relied upon. Many firms have horror stories of relying on certification and subsequently finding that it could not be relied upon.

- It's hard to say making compliance a requirement will not increase uptake. It may have a limited impact on reducing cyber issues. Many organisations who succumb to ransomware or other compromises are ISO compliant or have many other certifications. A further certification will not prevent this. For example, SolarWinds had SOC2 and ISO27001.

Part 3: Questions on Those Responding to the Call for Views

20. Are you responding as an individual or on behalf of an organisation?

    Organisation

21. [if individual] Which one of the following statements best describes you?
    - Cyber Security professional – Cyber Policy Advocacy for the Financial Sector

22. [if organisation] Which of the following statements best describes your organisation? (All selected below apply)
    a. Non-cyber security specific professional body or trade organisation with an interest in cyber security
    b. Financial Sector trade body representing over 300 organisations within the Banking and Finance space

23. [if organisation] Which one of the following best describes the sector of your organisation?
    a. Finance & insurance
    b. Other services

24. [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.

    250–999

25. [if organisation] What is the name of the organisation you are responding on behalf of? Free text

    UK Finance

26. Are you happy to be contacted to discuss your response and supporting evidence?

    Yes

27. [If yes] Please provide a contact name and email address below.
    Oge Udensi
    Policy Lead, Cyber and Third-Party Risk
    Oge.udensi@ukfinance.org.uk