CP/138 – Cross-Industry Guidance on Outsourcing

Executive summary

Google Cloud appreciates the efforts of the Central Bank of Ireland to refine cross-industry outsourcing rules and we welcome the opportunity to respond to the Consultation paper (CP) 138. Over the past several years, we have seen increased regulatory focus on harmonising the approaches to outsourcing and third-party risk management, including in the cloud context in Europe and globally.

The financial services industry is changing at a rapid pace, with shifting consumer expectations, new technologies, and continuously evolving regulatory requirements. Financial services firms need the right technology to help them stay agile and prepare for the future. The cloud has become a key point of leverage for firms looking to improve performance across a broad range of activities. Moving to the public cloud can advance operational resiliency, staff productivity, increase regulatory compliance, and enhance business model innovation.

As financial institutions (FIs) embark on their digital transformation journey all over the world, including in the view of the challenges brought on by the COVID-19 pandemic, we believe that clear and enabling principles for firms to use cloud services in a responsible way are key to regulators' overall objective to protect investors, ensure market integrity, and maintain financial stability.

Financial institutions are greatly benefiting from cloud technology in a multitude of ways to understand risk, segment customers, develop new instruments and ultimately offer better and more innovative products to their consumers. Thanks to the cloud, financial institutions can quickly process large volumes of information, reducing their time to market, and providing more agility and scalability at a lower cost. Capital markets firms can also utilise the cloud to combat fraud and money laundering through artificial intelligence (AI) and machine learning (ML) models. Similarly, cloud-based technologies are being leveraged for firms' risk-management to determine liquidity and exposure quicker, carry out mark-to-market adjustments and for more effective regulatory reporting. These benefits are fundamental to the industry transformation and need to be accounted for in the regulatory guidance.

FIs are choosing to use cloud services because they find the cloud to be equally or more secure and resilient than their existing, often legacy, computing infrastructure. The advancement and competition of cloud technologies in the last few years provide firms with data protection, data analytics, and operational resiliency capabilities that are more advanced than what individual organisations, especially SMEs and smaller firms, can develop on their own.

Our key observations from the Consultation Paper are as follows:

Firstly, we welcome the CBI's **general recognition of the benefits of public cloud and cloud-based services in the Consultation paper - in particular with a focus on their resilience and portability**. At the same time we note that the CP largely looks at public cloud from the perception of an increased risk - compared to utilising the on-premise datacentres. Whilst the regulator focus on risk mitigation is understandable, it is important to reflect on the reality of the modern cloud security and resilience model where migration to the public cloud infrastructure can provide more security and resilience capabilities - thanks to the cloud hyperscale technology and cyber expertise - than those available on premise.

Cloud customers also benefit from a variety of unique controls allowing them to have transparency over their data locality and providers' access to it, with robust security protections - largely by default - that are cost effective, meet international standards, and can fully address customer needs[1]. Our customers remain in control of their data and workloads, with Google Cloud providing both contractual commitments and technology tools to verify these guarantees[2]. Many of Google Cloud security innovations are deeply informed by the requirements of the European financial services customers.

Overall the security capabilities that are offered by hyperscale cloud providers have largely surpassed those available on premise, which is broadly recognised by the global financial services industry and regulatory authorities. In fact cloud's ability to augment security and reduce the risk is largely seen today as one of the reasons why regulated industries are accelerating their transition to the cloud[3]. From this perspective, we believe that the financial services institutions need to evaluate their cloud strategy with a focus on *risk management and mitigation*, and how their risk management processes can be improved with cloud functionality - not from a starting point of increased security or data privacy risk that is largely implied in the Consultation Paper.

Secondly, we welcome the very positive effort achieved by the CBI to **harmonise their outsourcing requirements with the existing European Supervisory Authorities (EBA, EIOPA, ESMA) Guidelines - as well as the PRA UK Outsourcing rules** which have been instrumental in stimulating further adoption of the new technology in a unified and clarified manner across Europe. This consistency is critically important to ensure that firms and their providers can effectively meet and manage their compliance

[1] https://cloud.google.com/security/overview/whitepaper
[2] https://cloud.google.com/blog/topics/inside-google-cloud/advancing-customer-control-in-the-cloud
[3] See McKinsey, Making a secure transition to the public cloud, 2018

obligations in the cross-border digital finance ecosystem. In addition, we agree it is extremely beneficial that the CBI harmonised the requirements to all financial services sector sub-verticals in the same Guidelines to avoid potential friction and fragmentation within the jurisdiction.

Thirdly, we note that whilst the Paper focused on a broad range of Outsourcing rules, there are certain **nuances in provision of cloud services which are multi-tenant** - meaning that the same services and datacentres are used by a multitude of customers, regulated and not, and all changes/requirements that apply to one service will be effectively implemented for all users regardless of the sector they represent. From this perspective, certain requirements in the CP are not proportionate or appropriate for cloud outsourcing as they would unintentionally create security, integrity and resilience vulnerabilities, for example:

- a requirement for the regulator to have access to customer encryption keys will pose a significant and disproportionate security risk;
- audit requirements in a multi-tenant environment such as public cloud need to account for associated risks and ensure that the audits do not create disruptions and collateral vulnerabilities for the integrity and resilience of cloud provider services and privacy of all their customers - whether they are subject to the Outsourcing rules or not;
- the same risks will be presented in the case of a public cloud provider participation in the BCP testing.

Finally, we welcome that the CBI takes a risk-based approach to data locality which is consistent with the ESAs Outsourcing Guidelines. However, we find the **restrictions on offshoring activities** not sufficiently clear and potentially concerning if they could impede the use of global technology and infrastructure by the Irish FIs.

We have provided detailed comments on these issues in our Consultation response.

We remain at your disposal for further discussion, and would welcome an opportunity to have a bilateral conversation to further substantiate our comments.

Detailed response

Question 1.	**Are there any aspects of the Guidance that are unclear? If so, please advise what these are and provide suggestions on the additional clarity required.**		
ref	**Draft Cross-Industry Guidance on Outsourcing**	**Google response**	**Google suggestion**
5.5(a)(i)	When considering or engaging in outsourcing to offshore jurisdictions, the Central Bank expects regulated firms to: a) Evaluate the particular risks associated with countries to which they are planning to outsource activities ensuring that their outsourcing risk assessments pay sufficient attention to 'country risk' and document the assessment. In assessing country risk, the Central Bank expects that regulated firms give consideration to and take steps to mitigate the following concerns and or risks: i. Regulatory environment – the strength and expertise of financial services regulatory regime in operation in the OSPs' jurisdiction;	**Issue** It is unclear why regulated firms should need to consider the strength and expertise of the financial services regulatory regime in the OSP's jurisdiction in all cases and not just where the performance of the outsourced function itself requires authorisation or registration by the Central Bank. Even if the function requires authorisation or registration, it is unclear why this assessment is required when offshoring to an EU Member State. **Rationale** Where the outsourced function does not itself require authorisation or registration by the Central Bank, the Central Bank would not have direct supervisory authority over the activity. Absent such authority, it is unclear why the local financial services regulatory regime is relevant. Equally, if the outsourced function does not require authorisation or registration it is unlikely that the local financial services regulatory regime will apply to the OSP directly. The EBA does not require an assessment of the local financial services regulatory regime unless the outsourcing function itself requires registration or authorisation and even then only for offshoring to third countries - see paragraph 63 of the EBA Outsourcing Guidelines. **Impact** Requiring regulated firms to make this assessment in all cases and even within the EU is unduly burdensome. It may also unduly restrict regulated entities from offshoring without a clear supervisory purpose.	We suggest that paragraph 5.5(a)(i) be amended as follows: i. Regulatory environment – if offshoring to a third country and only to the extent that the performance of the outsourced function requires authorisation or registration by the Central Bank, the strength and expertise of financial services regulatory regime in operation in the OSPs' jurisdiction;
5.5.1	Regulated firms may, if appropriate, be restricted from offshoring activities, where for example, supervisibility is either severely constrained or non-existent. Such constraints could arise where there is no College of Regulators, no Memorandum of Understanding (MoU) and little or no contact with regulators in the chosen jurisdiction. Additional constraints may result from the nature or location of any offshored activity, where this creates a barrier or impedes the ability of the Central Bank to appropriately supervise the activity, or where the operational risks associated with the offshoring of particular activities are deemed by the Central Bank to be excessive.	**Issue** The grounds for the Central Bank to restrict offshoring are not sufficiently clear. **Rationale** If the Central Bank is to have the power to restrict regulated firms from offshoring an activity, the criteria for exercising that power must be explicit. At present, the only limitation on the Central Bank exercising this power is if it is "appropriate" to do so. There are examples of when this may be the case, but they do not appear exhaustive. In addition, see above for discussion of the relevance of the offshore financial services regulatory regime. **Impact** Without clarity about when offshoring may be restricted, regulated firms will not have certainty about whether offshoring is / is not	We suggest that paragraph 5.5.1 be amended as follows: Regulated firms may, if appropriate, be restricted from offshoring activities, where ~~for example,~~ supervisibility is either severely constrained or non-existent. Such constraints could arise where the outsourced function requires authorisation or registration and there is no College of Regulators, no Memorandum of Understanding (MoU) and little or no contact with regulators in the chosen jurisdiction. Additional constraints may result from the nature or location of any offshored activity, where this creates a barrier or impedes the ability of the Central Bank to appropriately supervise the activity, or where the operational risks associated with the offshoring of particular activities are deemed by the Central Bank to be excessive.

		permitted. Nor will they be able to provide the Central Bank with the necessary information required under paragraph 5.5.1(a). This will put regulated firms in Ireland at a disadvantage compared to firms in other Member States, where these constraints do not exist.	
7.1(e)(ii)	The Central Bank expects that, with regard to the contract or written agreement (and associated SLAs) governing the provision of critical or important functions or services, these should be resolution resilient and set out in line with EBA Guidelines on Outsourcing and general good practice to include the following provisions: e) Whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and the conditions under which the sub-outsourcing is permitted. In this regard, the agreement should require OSPs to: i. notify regulated firms ahead of planned material changes to sub-outsourcing arrangements in a timely manner; ii. obtain prior specific or general written authorisation where appropriate; iii. give regulated firms the right to approve or object to material sub-outsourcing arrangements and/or terminate the agreement in certain circumstances; and iv. ensure that the regulated firm's and the Central Bank's rights of access and audit (see Section 8.3) apply in the case of any sub-outsourcing arrangement.	**Issue** The reference to specific or general authorisation should explicitly reference the relevant requirements in the GDPR. **Rationale** We believe this text is intended to reference Art 28 of the GDPR, which requires a processor to obtain specific or general authorisation from the controller to engage another processor. However, as written, this connection is not clear. The EBA makes this connection explicit at paragraph 78(d) of the EBA Outsourcing Guidelines. **Impact** Without clarification, this could inadvertently create an additional requirement that overlaps with the requirement at (iii) and is inappropriate in a public cloud context.	We suggest that paragraph 7.1(e)(ii) be amended as follows: ii. obtain prior specific or general written authorisation where appropriate before sub-outsourcing data*; *See Article 28 of Regulation (EU) 2016/679.
7.1(u)	The Central Bank expects that, with regard to the contract or written agreement (and associated SLAs) governing the provision of critical or important functions or services, these should be resolution resilient and set out in line with EBA Guidelines on Outsourcing and general good practice to include the following provisions: u) As a matter of good practice, regulated firms should also consider the inclusion of the following in contracts or written agreements: i. Dispute resolution arrangements containing provisions for remedies including penalty clauses to be invoked if required in the event of significant breaches of KPIs in respect of critical or important services;	**Issue** The Guidelines should not encourage regulated firms to include penalty clauses in their contracts with OSPs. **Rationale** Penalty clauses are unenforceable under Irish law. Remedies in service contracts typically take the form of service credits. **Impact** Unless clarified, this requirement will introduce confusion in contract negotiations.	We suggest that paragraph 7.1(u)(i) be amended as follows: i. Dispute resolution arrangements containing provisions for remedies including service creditspenalty clauses to be invoked if required in the event of significant breaches of KPIs in respect of critical or important services;
9(g) and (h)	When designing and implementing disaster recovery and business continuity measures as they pertain to or include outsourced arrangements, the Central Bank expects that regulated firms: (g) Ensure that they can participate in the OSPs business continuity plan testing, where necessary;	**Issue** Regulated firms and OSPs would benefit from more clarity on how the requirement to participate in / coordinate testing of business contingency plans (**BCP**) applies to public cloud. **Rationale** In the context of the shared responsibility model:	We suggest that paragraph 9(g) and (h) be amended as follows: (g) Ensure that they can participate in the OSPs business continuity plan testing, where appropriatenecessary;

	(h) Conduct coordinated testing of these arrangements on a regular basis and report the results to the boards of both the regulated firm and the OSP;	• Public cloud providers implement a BCP for the infrastructure, operations and resources required to provide their services. • Regulated firms implement a BCP for the outsourced process, service or activity. Firms can choose to use features or functionality of the cloud service to implement their own BCP (e.g. multi-regional/zonal architectures, back-up storage). Both parties test their own BCP. However, there are limits on what a public cloud provider can do to support an individual regulated firm's BCP testing given they provide a multi-tenant service. A public cloud provider can support a regulated firm's BCP testing as follows: • If the firm chooses to use cloud service features to implement or test its BCP, the provider can ensure those features are available and operate as expected during testing. • The provider can supply information and discuss best practices with firms for using their cloud services to implement the firm's BCP (e.g best practices for firms seeking to simulate the disruption of services they operate in the cloud). However, the following types of more direct involvement in testing in an individual firm's BCP testing would be problematic given the nature of public cloud services: • the provider cannot configure or deploy the cloud services on the firm's behalf to implement or test its BCP. This is inconsistent with the way cloud services operate. • the provider cannot simulate a disruption of its service to support a single firm's BCP testing. This could create undue risk for the provider's other customers. (However, cloud services do allow the firm to simulate a disruption themselves). **Impact** Without clarification these requirements may create expectations that are inconsistent with the operational realities of public cloud services and which introduce risk for the provider's other customers. We suggest adjusting the language to help to accommodate different service and delivery models. This is similar to the approach taken by the PRA at bullet 12 of paragraph 6.4 of SS2/21 Outsourcing and third party risk management.	(h) Where appropriate Conduct coordinated testing of these arrangements on a regular basis and report the results to the boards of both the regulated firm and the OSP;

Question 2.	**What, if any, are the other areas/topics that should be covered in the Guidance (specify sections) or in future versions of the Guidance?**		
ref	**Draft Cross-Industry Guidance on Outsourcing**	**Google response**	**Google suggestion**

7.3(d)	d) Regulated firms are expected to exercise their access and audit rights, determine the audit frequency and areas to be audited using a risk-based approach and in doing so adhere to relevant, commonly accepted, national and international audit standards.	**Issue** The Guidelines do not address important considerations for audit in the public cloud context. **Rationale** The ESAs have all recognised that additional considerations apply when conducting audits of multi-tenant environments like public cloud services. For example: • paragraphs 95 and 96 of the EBA Outsourcing Guidelines require reasonable advance notice and due care, respectively. • paragraph 41 of the EIOPA Guidelines on Outsourcing to Cloud Service Providers and paragraph 36 of the ESMA EIOPA Guidelines on Outsourcing to Cloud Service Providers recognise that if access or audit rights create a risk for OSP or its other customers, the parties should agree on alternative ways to provide similar assurance. These are important guardrails in the multi-tenant context where an audit by one customer necessarily introduces risks for the OSP's other customers. **Impact** The absence of these guardrails exposes other customers of the OSP (who may themselves be regulated firms) to undue risk.	We suggest that paragraph 7.3(d) be amended as follows: d) Regulated firms are expected to exercise their access and audit rights, determine the audit frequency and areas to be audited using a risk-based approach and in doing so adhere to relevant, commonly accepted, national and international audit standards. e) Before a planned on-site visit, regulated firms, competent authorities and auditors or third parties acting on each of their behalf should provide reasonable notice to the OSP, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective. f) When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated. If the exercise of its access or audit rights, or the use of certain audit techniques creates a risk for the environment of the OSP and/or another of the OSP's client, the regulated firm and the OSP should agree on alternative ways to provide a similar level of assurance and service to the regulated firm.

Question 3. What, if any, are the significant issues /or concerns or unintended consequences that might arise due to the provisions of the Guidance?

ref	Draft Cross-Industry Guidance on Outsourcing	Google response	Google suggestion
1(d)(iv)	In respect of the assessment of criticality or importance of activities or functions, the Central Bank expects that regulated firms: d) As criticality or importance may vary throughout the lifecycle of an outsourcing arrangement, the assessment of criticality or importance should be reviewed periodically in order to ensure the categorisations remain appropriate. It is recommended that such reviews be conducted at a minimum: (iv) if an organisational change at the OSP or a material sub-outsourced service provider takes place, including a change of ownership or to their financial position.	**Issue** A requirement to re-assess the criticality or importance of an outsourcing arrangement upon an organisational change at the OSP or a sub-outsourced service provider is disproportionate and does not align with the definition of materiality. **Rationale** As the Central Banks notes, functions that are necessary to perform core business lines or critical business functions should be considered as critical or important. The definition is focused on the importance of the function. Therefore, the position of the OSP should not be relevant to the assessment of whether the outsourcing itself is critical or important and, if so, how critical or important. The position of the OSP *is* relevant to whether they are *suitable* to perform critical or important outsourcing. However, this is separate from the question of criticality or importance itself and is already addressed by the obligation on the firm to monitor the outsourcing	**Option 1 (preferred)** We suggest that paragraph 1(d) be amended as follows: d) As criticality or importance may vary throughout the lifecycle of an outsourcing arrangement, the assessment of criticality or importance should be reviewed periodically in order to ensure the categorisations remain appropriate. It is recommended that such reviews be conducted at a minimum: ~~(iv) if an organisational change at the OSP or a material sub-outsourced service provider takes place, including a change of ownership or to their financial position.~~ **Option 2** We suggest that paragraph 1(d) be amended as follows:

		arrangement and the requirements at: • paragraph 5(e) and (f) on reviews and risk assessments of outsourcing arrangements • paragraph 7.1(k)(l) on reporting developments that have a material impact on the OSP's ability to effectively carry out the critical or important function • paragraph 7.1(e)(i) on material changes to sub-outsourcing. We suggest removing this reference entirely. However, if it is retained, we suggest: • it is linked the risks associated with the outsourcing arrangement; and • removing the references to "change of ownership" or "financial position", which are very broad (on a strict interpretation the service provider's ownership and financial position could change daily). These suggestions are consistent with EIOPA's approach at paragraph 25 of Guideline 7 of the EIOPA Guidelines on Outsourcing to Cloud Service Providers, which only requires undertakings to re-assess the criticality or importance if the nature, scale and complexity of the risks inherent in the agreement materially changes. They are also consistent with the PRA's approach at paragraph 5.8 of SS2/21 Outsourcing and third party risk management.	d) As criticality or importance may vary throughout the lifecycle of an outsourcing arrangement, the assessment of criticality or importance should be reviewed periodically in order to ensure the categorisations remain appropriate. It is recommended that such reviews be conducted at a minimum: (iv) if an organisational change at the OSP or a material sub-outsourced service provider takes place that materially changes the nature, scale and complexity of the risks inherent in the outsourcing arrangement~~, including a change of ownership or to their financial position~~.
5.2(b)(v)	In order to effectively manage risks relating to the potential loss, alteration, destruction or unauthorised disclosure of their sensitive data, the Central Bank expects regulated firms to: b) Have, as good practice, a documented data management strategy that addresses the range of risks, which can arise in the context of outsourcing including those relating to data transmission and storage including when offshored, which may give rise to heightened data protection concerns. The Central Bank expects the data management strategy to: v. ensure that, where data is encrypted, regulated firms make provisions to guarantee that any encryption keys or other forms of authentication are kept secure and accessible to the Central Bank; and	**Issue** A requirement that the Central Bank have access to encryption keys in the public cloud context is disproportionate and would introduce a serious, unnecessary security risk. **Rationale** Public cloud providers typically offer customers the ability to choose between customer-managed and provider-managed encryption. If a regulated firm chooses to use customer-managed encryption, then the regulated firm may make the relevant encryption keys available to the Central Bank as needed. If, however, a regulated firm chooses to use provider-managed encryption, then only the provider could provide the encryption keys. The provider uses the same encryption technology for all its customers. Many of these customers are not supervised by the Central Bank and in some cases could be supervised by a different competent authority. Requiring public cloud providers to share provider-managed encryption keys with the Central Bank introduces a security risk for all the provider's customers. This is disproportionate as the supervisory objective could be achieved without creating this risk if, instead of requiring that the Central Bank has access to the encryption keys, regulated firms were required to ensure that the	We suggest that paragraph 5.2(b)(v) be amended as follows: v. ensure that, where data is encrypted, regulated firms make provisions to guarantee that any encryption keys or other forms of authentication are kept secure and unencrypted data are accessible to the Central Bank; and

		Central Bank has access to the unencrypted data. Even where encryption is managed by the provider, Cloud services enable customers to access their data unencrypted. We note that the EBA does not require access to encryption keys. **Impact** As currently drafted, the Guideline will likely exclude regulated firms from using provider-managed encryption in the public cloud context as providers will be unable to provide the Central Bank with encryption keys without creating a serious, unnecessary security risk.	
	In order to monitor and manage this risk, the Central Bank expects regulated firms to: e) Evaluate elements of concentration risk and evidence such in the risk assessments and due diligence review when outsourcing critical or important functions. These considerations should include: i. Single firm concentration of multiple services at same OSP or intragroup service provider; ii. Lack of substitutability issue arising from single service provider in the marketplace; iii. Multiple number of regulated firms outsourcing to same OSP either on a sectoral or cross sectoral basis; iv. Concentration risk arising from chain outsourcing (sub-outsourcing/sub-contracting) arrangements; v. Concentration risk arising from outsourcing to offshore jurisdictions; and vi. Contribution to systemic outsourcing concentration risk, which the Central Bank is obliged to monitor from a financial stability perspective.	**Issue** It is disproportionate to require individual regulated firms to assess possible concentration within the sector. **Rationale** Individual firms do not possess the information needed to meaningfully assess concentration within the sector. OSPs are also unable to share confidential information about their relationship with one firm with any other firm. The Central Bank, however, will possess this information based on its supervision of all firms and are better placed to perform this assessment. **Impact** This could lead to firms attempting to perform a sector assessment without complete information and so arriving at conclusions that - at best - are not meaningful and - at worst - are counter-productive.	We suggest that paragraph 5.4(e) be amended as follows: In order to monitor and manage this risk, the Central Bank expects regulated firms to: e) Evaluate elements of concentration risk and evidence such in the risk assessments and due diligence review when outsourcing critical or important functions. These considerations should include: i. Single firm concentration of multiple services at same OSP or intragroup service provider; ii. Lack of substitutability issue arising from single service provider in the marketplace; ~~iii. Multiple number of regulated firms outsourcing to same OSP either on a sectoral or cross sectoral basis;~~ iv. Concentration risk arising from chain outsourcing (sub-outsourcing/sub-contracting) arrangements; v. Concentration risk arising from outsourcing to offshore jurisdictions; and vi. Contribution to systemic outsourcing concentration risk, which the Central Bank is obliged to monitor from a financial stability perspective.

9(d)	When designing and implementing disaster recovery and business continuity measures as they pertain to or include outsourced arrangements, the Central Bank expects that regulated firms: d) Consider the need for the creation of periodic isolated "safe harbour" backup arrangements in respect of cloud outsourcing arrangements as part of their business continuity planning, to ensure the preservation of data integrity and recovery in the aftermath of a major cyber event;	**Issue** This requirement is overly prescriptive and prevents the regulated firm from taking a risk-based approach. It may also be counterproductive from a disaster recovery and business continuity management perspective. **Rationale** Although it is appropriate for the Guidelines to require regulated firms to anticipate and mitigate specific risks, they should not dictate the measures regulated firms should take to mitigate those risks. Instead, the regulated firm should be able to define its own solutions taking a proportionate and risk-based approach. As an alternative to 'safe harbour' backups, regulated firms could address the risk of data loss / corruption by using measures available on the relevant cloud platform e.g. multiple storage options, out of region replication and highly durable archives. Equally, the regulated firm could choose to address this risk using a multi-cloud approach. Not only is a requirement for isolated "safe harbour" backup arrangements specifically for cloud outsourcing arrangements overly prescriptive, it is disproportionate to the management of similar risk on premise and seems to assume that cyber attacks or data loss are always more likely in the cloud than on premise. This is not the case. Indeed, from a technical perspective, Cloud platforms typically have more pervasive, integrated and up to date security mechanisms than firms' existing on-premise arrangements. The management of the Spectre and Meltdown vulnerabilities is a good illustration of this point. **Impact** The current prescriptive approach may be counterproductive from a disaster recovery and business continuity perspective. It could also discourage firms from moving their data to the cloud in the first place.	We suggest that paragraph 9(d) be amended as follows: d) Consider the need ~~for the creation of periodic isolated "safe harbour" backup arrangements in respect of cloud outsourcing arrangements~~ as part of their business continuity planning, to ensure the preservation of data integrity and recovery in the aftermath of a major cyber event;
Question 4. The Central Bank has considered existing sector specific legislation and guidance as they pertain to outsourcing and is of the view that this Guidance serves to provide additional clarity on the Central Bank's expectations and best practice when firms utilise outsourcing. Are there any particular aspects of the Guidance that appear to be at odds with existing sectoral requirements and could give rise to confusion/ misinterpretation? If so please provide details on any aspects which you believe may cause confusion and suggest how best to address such issues.			
	N/A	N/A	N/A