Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

This document is designed to help regulated firms supervised by the Central Bank of Ireland (“**regulated firm**”) to consider Cross Industry Guidance on Outsourcing (“**framework**”) in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: section 6 (Due Diligence), section 7 (Contractual Arrangement and Service Level Agreements), section 8 (Ongoing Monitoring and Challenge) and section 9 (Disaster Recovery and Business Continuity). For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	**6. Due Diligence**		
2.	The Central Bank expects that appropriate and proportionate due diligence reviews will be conducted in respect of all prospective OSPs or intragroup providers, before entering into any arrangements.	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below.	N/A
3.	With regard to critical and important functions, regulated firms should ensure that the OSP has the capabilities, and the appropriate authorisation, where required, to perform the critical or important function in a reliable and professional manner to meet its obligations over the duration of the contract.	See below.	N/A
4.	In respect of due diligence, the Central Bank expects that regulated firms consider the following criteria when conducting the initial due diligence review in respect of OSPs:		
5.	6. a) The OSPs business model, nature, scale, complexity, financial health, ownership and group structure;	You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct.	N/A
6.	6. b) The long-term relationships with OSPs that have already been assessed and perform services for the regulated firm;	This is a customer consideration.	N/A
7.	6. c) Whether the OSP is a parent undertaking or subsidiary of the regulated firm, is part of the accounting scope of consolidation of the regulated firm, is a member, or is owned by firms that are members of the same group. In this context i.e. intragroup arrangements, consideration should be given to the extent of control or influence which may be exercised by the regulated firm;	This is a customer consideration.	N/A
8.	6. d) Compliance with the General Data Protection Regulation (GDPR), Data Protection Act (DPA) and other applicable legal and regulatory requirements on data protection;	Google will comply with all national data protection regulations applicable to it in the provision of the Services. This is addressed in the Cloud Data Processing Addendum. For more information on how Google Cloud can assist you in complying with the GDPR see our GDPR resource center.	Representations and Warranties
9.	6. e) Whether the OSP is authorised by a regulatory authority to provide the service and whether or not the OSP is supervised by competent authorities;	Google is not subject to direct supervision by national competent authorities for Google Cloud services. However, Google will provide supervisory authorities with the assistance they need to review our Services.	Enabling Customer Compliance; Regulator Information, Audit and Access
10.	6. f) Capacity of the OSP to keep pace with innovation within the market sector;	Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance.	
11.	6. g) Business Reputation – including compliance, complaints and outstanding or potential litigation;	See above. In addition: You can review information about Google's historic performance of the services on our Google Cloud Status Dashboard. Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A
12.	6. h) Financial performance;	You can review Google's audited financial statements on Alphabet's Investor Relations page.	N/A
13.	6. i) Potential conflicts of interest, particularly in the case of intra-group arrangements ; and	This is a customer consideration.	N/A
14.	6. j) The effectiveness of risk management and internal controls, including IT and cybersecurity in providing appropriate technical and organisational measures to protect the data in accordance with the firm's Data Management Strategy as referenced in detail at Part B Section 5.2 above.	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page In addition, you can review Google's SOC 2 report.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. • Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
15.	In addition to the criteria listed above, the Central Bank expects that due diligence conducted by regulated firms also considers the:		
16.	6. a) Substitutability of the OSP/CSP (identifying possible alternative or back-up providers);	Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these	Data Export (Cloud Data Processing Addendum)

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	
17.	6. b) Potential exposure to concentration risk;	Google recognizes the importance of continuity for regulated firms and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A
18.	6. c) OSPs ability to demonstrate certified adherence to recognised, relevant industry standards;	You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
19.	6. d) Openness of the OSP to negotiating mutually acceptable contractual and SLA provisions	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	Enabling Customer Compliance
20.	6. e) Compatibility of the proposed arrangements with future development strategies of the regulated firm;	This is a customer consideration.	N/A
21.	6. f) Managerial skills of the regulated firm to oversee the OSP and the skills within the OSP;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account. Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	N/A
22.	6. g) Employment and management of sub-contractors by the OSP;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting	Google Subcontractors

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	
23.	6. h) Reliance by the prospective OSP on and control over sub-contractors;	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights).	Google Subcontractors
24.	6. i) Incident reporting and management programmes;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
25.	6. j) Insurance coverage;	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
26.	6. k) Resilience measures;	Google recognizes that resilience is a key focus for regulated firms and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it.	N/A
27.	6. l) Cross-border activities;	Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page.	N/A
28.	6. m) Track record of the OSP in respect of termination arrangements without having an impact on the continuity or quality of operations;	Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract.	Transition Term
29.	6. n) Ability of the OSP to meet its requirements and contractual obligations in relation to service quality and reliability, security and business continuity; in both normal and stressed circumstances;	Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues	Business Continuity and Disaster Recovery

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		to minimize the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper	
30.	6. o) Alignment of the risk appetite of the OSP with that of the regulated firm in order to avoid risk appetite breaches as a result of an OSP activity or failure. This may be avoided by both prior and ongoing assessment of the potential impact of outsourcing arrangements on operational risk appetite and risk tolerances as well as consideration of scenarios of possible risk events; and	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
31.	6. p) Design and effectiveness of risk management controls at the OSP being at least as strong as the controls utilised by the regulated firm itself (i.e. they should meet the regulated firms control objectives).	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001:2013 (Information Security Management Systems) -ISO/IEC 27017:2015 (Cloud Security) -ISO/IEC 27018:2014 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
32.	These criteria outlined above should also be considered, as deemed necessary, in the course of periodic reviews of due diligence throughout the lifecycle of any contract.	This is a customer consideration.	N/A
33.	**6.1 Values and Ethical Behaviour – Regulatory Expectations**		
34.	In line with EBA Guidelines on Outsourcing and general good practices, regulated firms are expected to		
35.	6.1 a) Take appropriate steps to ensure that OSPs act in a manner consistent with the values and code of conduct of the regulated firm; and	The Google Code of Conduct puts Google's values into practice. It's built around the recognition that everything we do in connection with our work at Google will be, and should be, measured against the highest possible standards of ethical business conduct.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Information about how Google operates its business in a sustainable way (including environmental information) is available on our Sustainability page. In addition, Google expects its suppliers to comply with the Google Supplier Code of Conduct.	
36.	6.1 b) Satisfy themselves, in particular with regard to OSPs located in third countries and if applicable, their sub-contractors, that the OSP acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.	See above.	N/A
37.	**6.2 Frequency of Due Diligence Review Performance**		
38.	With regard to the frequency of due diligence reviews, the Central Bank expects regulated firms to:		
39.	6.2 a) Conduct an initial due diligence review as outlined in this section, that covers the breadth of operational and financial capacity of the OSP to provide and maintain a quality service to the outsourcing regulated firm;	The information referenced above is available when you're performing your initial due diligence and throughout our relationship.	N/A
40.	6.2 a)b) Periodically review the "financial health" of key OSPs, providing critical or important services, over the lifecycle of the contract. Even the largest of the OSPs can fail; and	You can review Google's audited financial statements on Alphabet's Investor Relations page.	N/A
41.	6.2 a)c) Undertake / review a due diligence assessment prior to the expiry of key contracts in order to inform the decision of whether or not to renew the agreement. This should be performed sufficiently in advance of the termination / rollover date in order to permit the regulated firm sufficient time to either renegotiate the terms of the contract or undertake an orderly wind down or transfer of the arrangements.	See above.	N/A
42.	**7. Contractual Arrangements and Service Level Agreements (SLAs)**		
43.	The Central Bank expects that arrangements with OSPs are governed by formal contracts or written agreements, preferably that are legally binding. These should be supported by Service Level Agreements (SLAs). Intragroup arrangements should be implemented at a minimum by way of written agreements supported by SLAs. The adherence of OSPs whether external third parties or intragroup providers to contracts, written agreements and SLAs should be monitored by the regulated firm (see also Part B Section 8, which follows).	The Google Cloud Financial Services Contract is the written agreement between the parties. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page.	Services
44.	**7.1 General Requirements**		
45.	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,	The Google Cloud Financial Services Contract governs the provision of services to regulated entities.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	these should be resolution resilient and set out in line with EBA Guidelines on Outsourcing and general good practice to include the following provisions:		
46.	7.1 a) A clear description of the outsourced function or services to be provided;	Google Cloud services are described here.	Definitions
47.	7.1 b) The start date and end date (or renewal date, where applicable,) of the contract or agreement and the notice periods for the OSP and the regulated firm;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
48.	7.1 c) The governing law of the agreement i.e. the applicable jurisdiction for each agreement;	Refer to your Google Cloud Financial Services Contract.	Governing Law
49.	7.1 d) The parties' financial obligations;	Refer to your Google Cloud Financial Services contract. Prices and fee information are also publicly available on our SKUs page. Refer to our Pricing page for more information.	Payment Terms
50.	7.1 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:	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
51.	7.1 e) i. notify regulated firms ahead of planned material changes to sub-outsourcing arrangements in a timely manner;	See above.	N/A
52.	7.1 e) ii. obtain prior specific or general written authorisation where appropriate;	Google will comply with our obligations under the GDPR regarding authorization for subprocessing.	Processing of Data; Subprocessors (Cloud Data Processing Addendum)
53.	7.1 e) iii. give regulated firms the right to approve or object to material sub-outsourcing arrangements and/or terminate the agreement in certain circumstances; and	Refer to Row 50.	Google Subcontractors
54.	7.1 e) iv. ensure that the regulated firm's and the Central Bank's rights of access and audit (see Part B Section 8.3) apply in the case of any sub-outsourcing arrangement.	Google recognizes that chain-outsourcing must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
55.	7.1 f) Specify any functions or activities that are prohibited from being sub-outsourced;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would	Subcontracting; Google Subcontractors

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		potentially be denying all our customers the benefit motivating the subcontracting arrangement. To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice.	
56.	7.1 g) The location(s) (i.e. towns/cities, regions, and countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the regulated firm, in advance, if the OSP/CSP proposes to change the location(s);	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
57.	7.1 h) Where control/custody of data is being outsourced, requirements regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data. (These should provide for appropriate and proportionate information security related objectives and measures including requirements such as minimum cybersecurity requirements, specifications of firms' data life cycle, and any requirements regarding data security management, network security and security monitoring processes, operational and security incident handling procedures including escalation and reporting);	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
58.	7.1 i) Regulated firms should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes;	You can perform penetration testing of the Services at any time without Google's prior approval. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Customer Penetration Testing
59.	7.1 j) The right of the regulated firm to monitor the OSP's performance on an ongoing basis by reference to Key Performance Indicators (KPIs) which should be set out in the associated SLAs;	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Google Stackdriver** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring
60.	7.1 k) The agreed service levels, which should include precise quantitative (measureable) and qualitative performance targets (using KPIs to track) for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. In addition, if Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated firms may claim service credits.	Services
61.	7.1 l) The reporting obligations of the OSP to the regulated firm should require timely reporting against the KPIs, which provides actionable MI to the regulated firm. This should include communication by the OSP of any development that may have a material impact on the OSP's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, meeting the obligations to submit reports of the internal audit function of the OSP;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available here. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
62.	7.1 m) Whether the OSP should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
63.	7.1 n) The requirements (on all parties) to implement and test business contingency plans (taking account of the regulated firms impact tolerances for the disruption of critical or important services);	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Google is committed to enabling regulated entities to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article. We recognize that to remain within impact tolerances regulated entities often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud.	Business Continuity and Disaster Recovery
64.	7.1 o) Termination rights and exit strategies covering both stressed and non-stressed scenarios. As in the case of business contingency plans, both parties should commit to take reasonable steps to support the testing of regulated firms' exit strategies and termination plans – See also further detail relating to Termination Rights below;	Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here. For more information on transferring data on exit, refer to Row 154 - 164.	Data Export (Cloud Data Processing Addendum)
65.	7.1 p) Provisions that ensure that the data owned by the regulated firm can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the OSP/CSP;	Ownership You retain all intellectual property rights in your data. Insolvency Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to	Intellectual Property Term and Termination

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner.	
66.	7.1 p) a) to ensure resolution resiliency, for regulated firms, falling within scope of S.I. No. 289/2015 (the 2015 Regulations), which transposed Directive 2014/59/EU (BRRD) into Irish law, a clear reference to all relevant resolution authorities and the powers thereof especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD) as transposed by the relevant national competent authority, and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive; and for firms which are not subject to any current or likely future resolution framework, this Guidance should be considered good practice;	Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution.	Support through Resolution
67.	7.1 r) The unrestricted right of regulated firms and the Central Bank to inspect and audit the OSP/CSP with regard to, in particular, the critical or important outsourced function. See also Part B Section 7.3 Access, Information and Audit Rights below;	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
68.	7.1 s) Contractual arrangements, in respect of outsourcing, should ensure that where a situation of Recovery and or Resolution arises it cannot be deemed to be grounds for termination of the outsourcing arrangements in respect of critical or important services by the OSP;	See above	N/A
69.	7.1 t) Document the nature of the "shared responsibility" model (within the SLA) if such arises in the implementation of the cloud service arrangements. This should also document the agreed data management strategy and any restrictions on the offshoring of data; and	This is addressed in the Cloud Data Processing Addendum. We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers. It is important for regulated firms to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organization and the cloud service provider. Responsibility in the cloud is assigned as follows: • Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. • Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
70.	7.1 u) As a matter of good practice, regulated firms should also consider the inclusion of the following in contracts or written agreements:		
71.	7.1 u) 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;	Dispute resolution Refer to your Google Cloud Financial Services Contract. Corrective actions If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated firms may claim service credits.	Governing Law Services
72.	7.1 u) ii. Indemnification;	Google provides regulated firms with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.	Indemnification
73.	7.1 u) iii. Limits and liability;	Refer to your Google Cloud Financial Services Contract.	Liability
74.	7.1 u) iv. Provisions for amendment of contracts or written agreements; and	Refer to your Google Cloud Financial Services Contract.	Amendments
75.	7.1 u) v. Notifications of financial difficulty, catastrophic events, and significant incidents.	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.	Significant Developments
76.	7.2 **Termination Rights**		
77.	7.2 a) The contract or written agreement should expressly allow the possibility for the regulated firm to terminate the arrangement, in accordance with applicable law, including, inter alia, in the following situations:	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period, change of control or Google's insolvency. In addition, regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law, if directed by the competent authority or in any of the scenarios listed in Section 7.2.	Term and Termination
78.	7.2 a) i. where the OSP is in breach of applicable law, regulations or contractual provisions;	See above.	N/A
79.	7.2 a) ii. where impediments capable of altering the performance of the outsourced function are identified;	See above.	N/A
80.	7.2 a) iii. where there are material changes affecting the outsourcing arrangement or the OSP (e.g. sub-outsourcing or changes of sub-contractors);	See above.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
81.	7.2 a) iv. where there are weaknesses regarding the management and security of confidential, personal or other sensitive data or information e.g. a breach of agreed standards; and	See above.	N/A
82.	7.2 a) v. where instructions to terminate are given by the Central Bank, e.g. in the case that the Bank is, as a consequence of the outsourcing arrangement, no longer in a position to effectively supervise the regulated firm.	See above.	N/A
83.	7.2 b) The contract or written agreement governing the outsourcing arrangement should facilitate the transfer of the outsourced function to another OSP or its re-incorporation into the regulated firm. Consequently, the contract or written agreement should:		
84.	7.2 b) i. clearly set out the obligations of the existing OSP, in the case of a transfer of the outsourced function to another OSP or back to the regulated firm, including the treatment of data;	Google will enable you to access and export your data throughout the duration of our contract. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Cloud Data Processing Addendum)
85.	7.2 b) ii. set an appropriate transition period, during which the OSP, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and	Google recognizes that institutions need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help institutions achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract.	Transition Term
86.	7.2 b) iii. include an obligation on the OSP to support the regulated firm in the orderly transfer of the function in the event of the termination of the outsourcing agreement.	Our Services enable you to transfer your data independently. You do not need Google's permission to do this. Refer to Row 84. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Assistance
87.	7.3 **Access, Information and Audit Rights**		
88.	7.3 a) Regulated firms should ensure within the contract or written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.	Google grants audit, access and information rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.	Customer Information, Audit and Access

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
89.	7.3 b) The contract or written outsourcing arrangements, regardless of the criticality or importance of the outsourced function, should refer to the information gathering and investigatory powers of competent authorities and resolution authorities, as applicable, with regard to OSPs located in a Member State and should also ensure those rights with regard to OSPs located in third countries.	Google acknowledges the information gathering and investigatory powers under the relevant EU Directives.	Enabling Customer Compliance
90.	7.3 c) Regulated firms should ensure that within the contract or written outsourcing agreement, with regard to the outsourcing of critical or important functions the OSP grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Regulator Information, Audit and Access; Customer Information, Audit and Access
91.	7.3 c) i. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the OSP's external auditors ('access and information rights'); and	See above.	N/A
92.	7.3 c) ii. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.	See above.	N/A
93.	7.4 **Review of Agreements**		
94.	7.4 a) Written agreements and contracts should be reviewed periodically, for example, when changes to the business model, the completion of risk assessments or regulatory change, warrants a reconsideration of the continued suitability of the contract.	This is a customer consideration.	N/A
95.	7.4 b) Reviews should also be scheduled in sufficient time in advance of renewals or termination dates to ensure smooth transitions or continuity of service.	This is a customer consideration.	N/A
96.	7.5 **Non-Critical or Important Outsourcing Arrangements**		
97.	7.5 a) Written agreements for non-critical or less important outsourcing arrangements should include appropriate contractual safeguards to manage relevant risks.	Google recognizes that use of the Services could scale up over time. Regardless of how regulated entities choose to use the Services at the start of our relationship, Google will provide regulated entities and supervisory authorities with information, audit, and access rights.	Enabling Customer Compliance
98.	7.5 b) Regardless of criticality or importance, regulated firms should ensure that outsourcing agreements/contracts do not impede or limit the Central Bank's (or third parties appointed by it to exercise these rights) ability to effectively supervise or audit the regulated firm or its outsourced activity, function or service.	Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively.	Enabling Customer Compliance
99.	8. **Ongoing Monitoring and Challenge**		
100.	In conducting appropriate monitoring and challenge of the outsourcing framework, the underlying outsourcing arrangements and the operational functioning of same, regulated firms should incorporate outsourcing assurance into its three lines of defence.	This is a customer consideration.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
101.	8.1 **Monitoring of outsourcing arrangements**		
102.	Regulated firms are expected to put in place appropriate mechanisms to oversee, monitor, and assess the appropriateness and performance of their outsourced arrangements. Such mechanisms will generally be executed by the first line of defence with oversight and challenge through the second line in terms of performance against standards and effective management of the risk. In this regard, the Central Bank expects that regulated firms:		
103.	8.1 a) Have sufficient and appropriately skilled staff within the organisation to oversee, interrogate, analyse and challenge the effectiveness of the outsourced arrangement (in line with Part B Section 4.1 (g) above);	Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications. Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
104.	8.1 b) Identify key decision makers who have the ability and capability to make decisions based on the information being provided;	This is a customer consideration.	N/A
105.	8.1 c) Monitor the performance of the OSP using a risk based approach, including by:	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The Status Dashboard provides status information on the Services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring.
106.	8.1 c) i. Ensuring receipt of appropriate reports from the OSP;	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis.	Significant Developments

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
107.	8.1 c) ii. Assessing the performance of the OSP, including through the use of measures agreed and documented in their SLAs e.g. key performance indicators (KPIs), key control indicators (KCIs), service reviews and reports, outcomes of internal audit or other third party independent reviews commissioned by the OSP;	Performance measures The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. Audit reports Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Services Certifications and Audit Reports
108.	8.1 c) iii. Assessing the adequacy of the OSPs business continuity measures and associated testing and the effectiveness of the integration with those of the firm, as detailed in Part B Section 10 below; and	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated firms can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
109.	8.1 c) iv. Conducting onsite reviews of the OSP.	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Regulator Information, Audit and Access; Customer Information, Audit and Access
110.	8.1 d) Take appropriate measures to ensure that any deficiencies identified in the provision of the service by the OSP are effectively addressed, and if necessary escalated to ensure remediation. This may include an ultimate decision to terminate the arrangement; and	Google is committed to taking appropriate corrective or remedial actions if an audit on behalf of the regulated entity or the supervisory authority identifies unaddressed deviations in the Services operations and controls.	Customer Information, Audit and Access; Regulator Information, Audit and Access
111.	8.1 e) Incorporate assurance testing related to the management and monitoring of outsourcing as part of their risk management and compliance monitoring programmes. Such monitoring reviews as referred to above and assurance testing should be conducted on a frequency and to a degree commensurate with the nature, extent and criticality of the outsourcing arrangements engaged in by the regulated firms and its outsourcing risk assessment in respect of each of these arrangements. Firms should document the rationale, in its Outsourcing Policy, for the selected frequency of the conduct of such reviews and be in a position to provide this information to supervisors on request.	The regulated entity is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit regulated entities to a fixed number of audits or a pre-defined scope.	Customer Information, Audit and Access
112.	8.2 **Internal Audit & Independent Third Party Review**		
113.	Part B Section 8.1 above, refers to the day-to-day operational oversight of the performance of the OSP by the first and second line of defence. Regulated firms must also ensure that assessment of the effective performance of the arrangement and of the controls to mitigate associated risks, forms part of its third line of defence assurance programme, via its internal audit plan. In line with their outsourcing policy and risk assessment, regulated firms should also consider the circumstances in which independent external third party review may be necessary, in order to obtain satisfactory assurance regarding their outsourcing universe. The Central Bank expects that:	The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment. In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Board of Directors Handbook for Cloud Risk Governance and Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud.	N/A
114.	8.2 a) Using a risk based approach, the audit programme of the internal audit function assesses:	See above.	N/A
115.	8.2 a) i. That the regulated firm's outsourcing framework is operating effectively and in line with the outsourcing policy and the firm's risk appetite;	See above.	N/A
116.	8.2 a) ii. Whether the outsourcing policy and associated control framework have been reviewed and updated to take account of any changes to the business, any new or	See above.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	emerging risks and any changes to the legislative or regulatory framework that impact on the firm's outsourcing universe;		
117.	8.2 a) iii. That outsourcing arrangements are being correctly classified in line with the regulated firm's methodology for the assessment of "criticality and importance". In this context, periodic assessment of the firm's methodology should also be conducted to ensure that it remains appropriate and fit for purpose, based on the firms business model, strategy and risk assessment;	See above.	N/A
118.	8.2 a) iv. That the regulated firm's outsourcing register is being appropriately maintained to ensure accuracy and currency;	See above.	N/A
119.	8.2 a) v. The adequacy and appropriateness of the firm's outsourcing risk assessment generally and it's application in respect of specific outsourcing arrangements;	See above.	N/A
120.	8.2 a) vi. The effectiveness of the oversight and direction of the board, senior management or management body and any relevant committees in respect of outsourcing;	See above.	N/A
121.	8.2 a) vii. The effectiveness of the regulated firm's monitoring and management of its outsourcing arrangements; and	See above.	N/A
122.	8.2 a) viii. The operation by the OSP of the underlying outsourced activities or functions via onsite audits.	Google grants audit, access and information rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.	Customer Information, Audit and Access
123.	8.2 b) Regulated firms ensure that the party conducting the audit/review, whether internal or external, has the necessary skills and expertise to conduct the review effectively and to comprehensively assess and report on the outcomes. This is of particular relevance where the outsourcing arrangement presents a significant degree of technical complexity, for example in the case of outsourcing to cloud service providers (CSPs).	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
124.	8.2 c) Regulated firms ensure that they have the appropriate skills and expertise to review, challenge and make informed decisions as to the quality and outcomes of any audit/review.	See above.	N/A
125.	8.3 **Use of Third Party Certifications and Pooled Audits**		
126.	As part of their ongoing monitoring regime, regulated firms may utilise a number of different sources of information to aid their awareness and understanding of risks associated with their outsourcing arrangements and how these risks are managed. This may include independent third party reports and certifications provided by the OSP and onsite audits of the activities of the OSP. Onsite audits may be conducted by the internal audit function or a third party commissioned directly by the regulated firms (as	Third Party Reports and Certifications Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:	Certifications and Audit Reports

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	referenced in Part B Section 8.2 above), or in appropriate circumstances onsite audits may also be conducted with other regulated firms (pooled audits). Where regulated firms utilise third party certifications provided by the OSP and/or pooled audits, the Central Bank expects that:	• ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Onsite Audits Google recognizes that regulated firms and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated firms, supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit. Pooled Audits Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.	Regulator Information, Audit and Access Customer Information, Audit and Access N/A
127.	8.3 a) Regulated firms assess and document the circumstances in which third party certifications and pooled audits are deemed to provide appropriate levels of assurance, in line with their outsourcing policy and risk assessment. In this context, regulated firms must be mindful that the level of assurance required may be more onerous given the nature, scale and complexity of their business and the criticality and importance of the outsourced functions that are the subject of the review.	This is a customer consideration.	N/A
128.	8.3 b) When utilising third party reports or certifications or availing of pooled audits, the regulated firm is satisfied and can evidence that:		
129.	8.3 b) i. The scope and process for the review is appropriate, and provides sufficient coverage of the outsourced activities and functions and related risk management controls;	As relates to Google's third party certifications and audit reports, Google's audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope.	Certifications and Audit Reports

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
130.	8.3 b) ii. The review criteria are up to date and take account of all relevant legal and regulatory requirements;	As relates to Google's third party certifications and audit reports, as part of Google's routine planning, scoping, and readiness activities, recurring key systems and controls, as well as new systems and controls, are reviewed prior to the audit work commencing.	Certifications and Audit Reports
131.	8.3 b) iii. The third party commissioned to conduct the review has the appropriate skills and expertise (in line with the general requirements relating use of independent third parties referenced in Part B Section 8.2 above); and	As relates to Google's third party certifications and audit reports, Google engages certified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the certifying or auditing party.	Certifications and Audit Reports
132.	8.3 b) iv. The regulated firm has the appropriate skills and expertise to review, challenge and make informed decisions as to the quality and outcomes of the review (in line with the general requirements relating use of independent third parties referenced in Part B Section 8.2 above).	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
133.	8.3 c) Regulated firms ensure that their audit methodology enables them to fulfil their legal and regulatory obligations at all times, in particular as they relate to outsourcing risk management and operational resilience.	This is a customer consideration.	N/A
134.	9. **Disaster Recovery and Business Continuity Management**		
135.	Key to effective governance and risk management associated with any outsourcing arrangement is ensuring continuity of services through robust disaster recovery (DR) and business continuity management (BCM). An integral part of the DR/BCM process is the regulated firm's resilience to an event occurring. Critical to this is the continuous assessment of the regulated firm's business processes and the DR and business continuity plans (BCPs) in place, to ensure that controls or other resilience measures are effective and in line with evolving practice and emerging risks and/or issues.	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications	N/A
136.	In order to ensure the robustness of a regulated firm's own DR and business continuity plans (BCPs), it is important that regulated firms consider the implications of having outsourced to an OSP and the BCM arrangements that the OSP has in place. It is important that there is close alignment of the DR/BCM arrangements of regulated firms and those of their outsource service providers (OSP), particularly where the OSP is	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own	Business Continuity and Disaster Recovery

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	involved in the delivery of critical or important functions and their related systems and data.	business contingency planning is available in our Disaster Recovery Planning Guide.	
137.	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:		
138.	9. a) Consider DR/BCM when proposing to engage the services of an OSP and ensure that service disruptions can be maintained within the impact tolerances and recovery time objectives (RTOs) of the firm as documented within its most recent Business Impact Analysis;	Google recognizes that regulated entities are expected to set impact tolerances on the assumption that a disruption will occur. Google is committed to enabling regulated entities to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article. We recognize that to remain within impact tolerances regulated entities often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud.	N/A
139.	9. b) Ensure that when entering into an outsourcing arrangement, all governance surrounding such an arrangement, including business continuity plans and exit strategies (see Part B Section 9.1) are updated to reflect any implications of the outsourcing arrangement;	See above.	N/A
140.	9. c) Document and implement business continuity plans in relation to their critical and important outsourced functions and that these plans are tested and updated on a regular basis.	See above.	N/A
141.	9. 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;	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google’s approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	
142.	9. e) Ensure the OSP has a business continuity plan in place, which includes the resources (processes, systems, personnel etc.) required to fulfil the regulated firm's critical or important outsourcing arrangements;	Google's business continuity plan describes Google's business continuity and disaster recovery strategy, methodology, and testing programs. The business continuity plan is designed to cover key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware.	Business Continuity and Disaster Recovery
143.	9. f) Ensure that any critical or important outsourcing arrangement includes a requirement for the OSP to carry out testing of its own business continuity plans at least annually;	Google recognizes the importance of regular testing in the context of operational resilience. Google runs annual, company-wide, multi-day Disaster Recovery Testing events (DiRT) to ensure that Google's services and internal business operations continue to run during a disaster. DiRT was developed to find vulnerabilities in critical systems by intentionally causing failures, and to fix those vulnerabilities before failures happen in an uncontrolled manner. DiRT tests Google's technical robustness by breaking live systems and tests our operational resilience by explicitly preventing critical personnel, area experts, and leaders from participating. All generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability. Refer to this blog post for more information about the resilience testing that Google performs as well as recommendations on how to train your first responders so they can react efficiently under pressure. You'll also find templates so you can get started testing these methods in your own organization. Firms can also request to review Google Cloud's testing results.	Business Continuity and Disaster Recovery
144.	9. g) Ensure that they can participate in the OSPs business continuity plan testing, where necessary;	In addition to testing our own environments, Google also provides a number of tools and resources that enable firms to independently test their Google Cloud deployments. Our Disaster Recovery Scenarios for Data and Disaster Recovery for Applications articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively. You can also implement the following to help with your own testing: • Automate infrastructure provisioning with Deployment Manager. You can use Deployment Manager to automate the provisioning of VM instances and other Google Cloud infrastructure. If you're running your production environment on premises, make sure that you have a monitoring process that can start the disaster recovery process when it detects a failure and can trigger the appropriate recovery actions.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Monitor and debug your tests with Cloud Logging and Cloud Monitoring. Google Cloud has excellent logging and monitoring tools that you can access through API calls, allowing you to automate the deployment of recovery scenarios by reacting to metrics. When you're designing tests, make sure that you have appropriate monitoring and alerting in place that can trigger appropriate recovery actions.	
145.	9. 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;	See above.	N/A
146.	9. i) Have sight of reports on business continuity measures and testing undertaken by the OSP and are informed of any relevant actions or remediation arising as a result of this testing, as appropriate;	See above.	N/A
147.	9. j) Ensure that boards and senior management of the firm take remedial action to address any deficiencies identified in the performance of the OSP, either as part of coordinated testing of the regulated firm's business continuity measures, or via results of the OSP's own BCP testing. Such actions may include ultimate termination of the outsourced arrangement if such deficiencies persist;	This is a customer consideration.	N/A
148.	9. k) Regularly review the appropriateness of their business continuity plans and resilience measures in respect of outsourced activities, particularly in the context of new and evolving technologies, trends and risks;	This is a customer consideration.	N/A
149.	9. l) Ensure that outsourcing arrangements are considered in the context of firms' recovery planning and resolution planning and that the operational continuity of critical functions is ensured including scenarios of financial distress or during financial restructuring or resolution.	This is a customer consideration.	N/A
150.	When considering appropriate DR/BCP measures these considerations should be linked with the planning of Exit Strategies – See Part B Section 9.1, which follows.	This is a customer consideration.	N/A
151.	9.1 **Exit Strategies**		
152.	The resilience of any regulated firm to vulnerabilities presented by outsourcing arrangements will be largely dictated by the effectiveness of the contingency measures in place, including their exit strategies. As outsource service users, regulated firms should understand exit costs, the arrangements to be initiated and the legal and operational risk implications in the event of the termination of outsourcing contracts or arrangements whether with third parties or intragroup.	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk.	N/A
153.	When entering into an outsourcing arrangement, the Central Bank expects regulated firms to consider and plan how the regulated firm would exit the arrangement for example in the case of:		

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
154.	9.1 a) Failure on the part of the OSP to provide the service to the requisite standard;	Google recognizes that, whatever the level of technical resilience that can be achieved on Google Cloud, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: • **Commitment to Open Source:** many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. • **Commitment to common standards:** our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. • **Anthos multi-Cloud management:** our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on Google Cloud across other Cloud providers or on-premise. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	Data Export (Cloud Data Processing Addendum)
155.	9.1 b) Unexpected termination of the arrangement dictated by the OSP/CSP;	See above.	N/A
156.	9.1 c) Stressed circumstances on the part of the OSP such as hostile takeover, insolvency or liquidation; or	Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to	Data Export (Cloud Data Processing Addendum) Term and Termination

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner.	
157.	9.1 d) Any other circumstance that the regulated firm envisages may prompt it to exit the arrangement.	See above.	N/A
158.	With regard to the development and maintenance of exit strategies associated with outsourcing arrangements, the Central Bank expects that regulated firms:		
159.	9.1 a) Have considered and documented their impact tolerances for business service interruptions and have in place a documented framework to identify and escalate breaches of these tolerances and procedures for dealing with same. This framework, (which may be linked to monitoring of performance against SLAs as detailed in Part B Sections 7 and 8 respectively), should include criteria and procedures for invoking an exit strategy where deemed necessary;	Google recognizes that regulated entities are expected to set impact tolerances on the assumption that a disruption will occur. Google is committed to enabling regulated entities to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article. We recognize that to remain within impact tolerances regulated entities often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud.	N/A
160.	9.1 b) Have a clearly defined and documented exit strategy in place (in particular for their critical or important outsourcing arrangements), which is viable, appropriately planned, documented and regularly tested and takes into account at least the circumstances detailed in Part B Section 9.1 above;	Refer to Row 154.	N/A
161.	9.1 c) Assess whether an OSP can be substituted. Where substitutability is established, regulated firms should seek to identify alternate OSPs and make appropriate assessments of the measures required to transfer to such alternate providers where an exit strategy must be invoked. Theses assessments should inform the regulated firm's exit strategy;	Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	Data Export (Cloud Data Processing Addendum)
162.	9.1 d) Ensure that the exit strategy includes arrangements for reintegration of services within the regulated firm or group entity, either where an alternative provider is not available or in cases where reintegration is required by regulation;	See above.	N/A

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
163.	9.1 e) Consider, plan and test (insofar as is possible) scenarios which may warrant the transfer of activities to another OSP or back in-house;	Google will enable you to access and export your data throughout the duration of our contract. You can export your data from the Services in a number of industry standard formats. For example: • **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Cloud Data Processing Addendum)
164.	9.1 f) Develop and maintain skills and expertise so that functions can, if required, be taken back in- house by the regulated firm or transferred to an alternative provider in an orderly manner;	This is a customer consideration.	N/A
165.	9.1 g) Ensure that the exit strategy estimates the timeframe for transfer of service either to an alternative provider, or if necessary, to take the service back in–house;	Google recognizes that regulated firms need sufficient time to exit our services (including to transfer services to another service provider). To help regulated firms achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract.	Transition Term
166.	9.1 h) Consider and implement within their exit strategy, contingency arrangements to cover the interim period between invoking an exit strategy and the ultimate transfer. This is particularly important where the timeframe for transfer of service is significant;	See above.	N/A
167.	9.1 i) Ensure appropriate understanding and oversight of the data flows between the regulated firm and the OSP, including how to manage any potential interruption of service or downtime to ensure that critical business functions remain available;	Refer to Row 159 and 163.	N/A
168.	9.1 j) Have considered the potential for and implications of "step-in risk" materialising in the context of stressed scenarios. Regulated firms should determine the viability of invoking 'step-in' rights in such scenarios. The form that such 'step-in' would take should be determined, which may include providing financial support for, or takeover of the OSP. Where 'step-in' is deemed viable, it should be planned and documented as part of the exit strategy;	This is a customer consideration. You can review Google's audited financial statements on Alphabet's Investor Relations page.	N/A
169.	9.1 k) Periodically review and update exit strategies to take account of developments that may alter the feasibility of an exit in stressed or non-stressed circumstances. For example, new service providers or new technology tools which, particularly in the case of cloud outsourcing arrangements, may facilitate switching of service providers or locations and the portability of critical data and applications. These tools are constantly evolving, in particular in technology outsourcing, including Cloud, and may include:	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk.	Data Export (Cloud Data Processing Addendum)

Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	
170.	9.1 k) i. evaluation of new potential OSPs;	See above.	N/A
171.	9.1 k) ii. technology solutions and tools to facilitate the switching and portability of data and applications; and	See above.	N/A
172.	9.1 k) iii. adoption and adherence to industry codes and standards by the provider;	Google complies with the SWIPO (Switching Cloud Providers and Porting Data) Data Portability Codes of Conduct. For more information refer to our SWIPO Data Portability Code of Conduct page.	N/A
173.	9.1 l) In the specific case of critical or important cloud outsourcing arrangements, assess the resilience requirements of the outsourced service and data and determine which of the available Cloud resiliency service options is most appropriate. These may include multiple availability zones, regions or service providers;	Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes.	N/A
174.	9.1 m) Ensure that in the case of intra-group arrangements, where regulated firm's avail of exit plans that have been established at a group level, that the plans address the expectations set out in this Guidance and relevant sectoral legislation and regulatory requirements. Regulated firms must ensure that such plans are viable and can be executed accordingly in respect of the regulated firm's critical or important outsourced arrangements.	This is a customer consideration.	N/A