FCA - FG 16/5

Google Workspace Mapping

This document is designed to help firms supervised by the Financial Conduct Authority ("**regulated entity**") to consider FG 16/5 Guidance for firms outsourcing to the "cloud" and other third-party IT services (the "**framework**") in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the areas firms should consider in relation outsourcing to the cloud and other third-party IT services. 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.	**Legal and regulatory considerations**		
2.	Before acceptance, firms should review the contract with the outsource provider to ensure that it complies with our requirements. A firm should:		
3.	• have a clear and documented business case or rationale in support of the decision to use one or more service providers for the delivery of critical or important operational functions or material outsourcing;	This is a customer consideration.	N/A
4.	• ensure the service is suitable for the firm and consider any relevant legal or regulatory obligations, including where a firm is looking to change their existing outsourcing requirements;	This is a customer consideration.	N/A
5.	• as part of the due diligence exercise, ensure that in entering into an outsource agreement, it does not worsen the firms operational risk;	You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities and can configure the service to avoid undue operational risk. For more information about Google's approach to risk and security, refer to Row 37.	N/A
6.	• consider the relative risks of using one type of service over another e.g. public versus private cloud;	This is a customer consideration.	N/A
7.	• maintain an accurate record of contracts between the firm and its service provider(s);	This is a customer consideration.	N/A
8.	• know which jurisdiction the service providers business premises are located in and how that affects the firms outsource arrangements;	For more information about the location of Google's facilities and where individual Google Workspace services can be deployed, refer to Row 38.	N/A
9.	• know whether its contract with the service provider is governed by the law and subject to the jurisdiction of the United Kingdom. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and relevant regulator (see below sections on access to data and business premises);	Refer to your Google Cloud Financial Services Contract. For more information on data access and audit rights (including on-site audits), refer to Row 58.	Governing Law
10.	• consider any additional legal or regulatory obligations and requirements that may arise such as through the General Data Protection Regulation (GDPR);	For more information on how Google Cloud can assist you in complying with the GDPR see our GDPR resource center.	N/A
11.	• where these are related to the regulated activity being provided, identify all the service providers in the supply chain and ensure that the requirements on the firm can be complied with throughout the supply chain. Similarly, where multiple providers form part of an overall arrangement (as distinct from a chain) the requirements should be complied with across the arrangement.	For more information about Google subcontractors and accountability refer to Row 75.	N/A
12.	**Risk management**		

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
13.	A fundamental principle of the rules and guidance on outsourcing is that firms identify and manage any risks introduced by their outsourcing arrangements. Accordingly, firms should:		
14.	• carry out a risk assessment to identify relevant risks and identify steps to mitigate them;	This is a customer consideration.	N/A
15.	• document this assessment;	This is a customer consideration.	N/A
16.	• identify current industry good practice, including data and information security management system requirements, cyber risks, as well as the relevant regulators rules and guidance to then use this to support its decision making;	This is a customer consideration.	N/A
17.	• review whether the legal and regulatory risks differ if the customers, firms and employees involved in providing or using the services are in different geographic or jurisdictional locations e.g. UK, EEA or non-EEA;	For more information about the location of Google's facilities and where individual Google Workspace services can be deployed, refer to Row 38.	N/A
18.	• assess the overall operational risks associated with the regulated service for which the firm is responsible and assign responsibility for managing them;	This is a customer consideration.	N/A
19.	• monitor concentration risk and consider what action it would take if the outsource provider failed;	This is a customer consideration. For more information on the substitutability of our services refer to Row 94.	N/A
20.	• require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements;	For more information on incident notification, refer to Row 39.	N/A
21.	• ensure the contract(s) provide for the remediation of breaches and other adverse events.	Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period.	Term and Termination
22.	**International standards**		
23.	In conducting its due diligence on potential third-party providers, and as part of ongoing monitoring of service provision, a firm may wish to take account of the providers adherence to international standards as relevant to the provision of IT services. Assurance obtained from international standards for the delivery of critical or important operational functions or material outsourcing is unlikely to be sufficient on its own. Nevertheless, firms should:	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) • SOC 1 • SOC 2 • SOC 3	Certifications and Audit Reports

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24.	• take account of any external assurance that has already been provided when conducting their own due diligence.	You can review Google's current certifications and audit reports at any time.	N/A
25.	External assurance may be more relevant to a firm's consideration where:		
26.	• it complies to well-understood standards (such as, for example, the ISO 27000 series);	For more information on the international standards Google Cloud complies with, refer to Row 23.	Certifications and Audit Reports
27.	• the part of the service being assessed is relatively stable (such as physical controls in the data centre or staff vetting);	This is a customer consideration.	N/A
28.	• the service is uniform across the customer base (i.e. not particular or bespoke to the firm outsourcing);	Google provides the same services to all customers using a common technical platform and a common set of tools.	N/A
29.	• the scope of the third-party audit is specific to the service a firm proposes to use (i.e. the audit is against the data centre you are using not a similar data centre in another jurisdiction).	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. The precise scope of our certifications and audit reports is described in the relevant certification or report.	N/A
30.	**Oversight of service provider**		
31.	Firms retain full accountability for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider. At a high level, a firm should:		
32.	• be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends;	The Google Workspace services are described on our services summary page. The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	Definitions
33.	• allocate responsibility for the day-to-day and strategic management of the service provider;	This is a customer consideration.	N/A
34.	• ensure staff have sufficient skills and resources to oversee and test the outsourced activities; identify, monitor and mitigate against the risks arising; and properly manage an exit or transfer from an existing third-party provider;	Skills and resources 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. Monitoring	N/A Ongoing Performance Monitoring

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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). Exit and transfer services For more information on exit or transfer, refer to Row 94.	
35.	• verify that suitable arrangements for dispute resolution exist.	Refer to your Google Cloud Financial Services Contract.	Governing Law
36.	**Data security**		
37.	Firms should carry out a security risk assessment that includes the service provider and the technology assets administered by the firm. A firm should:	The security of a cloud service consists of two key elements: 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.	Data Security; Security Measures (Data Processing Amendment)

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. 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 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. (b) Security resources Google also publishes guidance on: • Security best practices • Security use cases	
38.	• agree a data residency policy with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm's data can be stored, processed and managed. This policy should be reviewed periodically;	Data center locations 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 Workspace services can be deployed is available here. • Information about the location of Google's subprocessors' facilities is available here.	Data Transfers (Data Processing Amendment)

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Data storage 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 Security; Subprocessors (Data Processing Amendment) Data Location (Service Specific Terms)
39.	• understand the provider's data loss and breach notification processes and ensure they are aligned with the firm's risk appetite and legal or regulatory obligations;	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 (Data Processing Amendment)
40.	• consider how data will be segregated (if using a public cloud);	To keep data private and secure, Google logically isolates each customer's data from that of other customers. For more information on Google's security infrastructure, refer to Row 37.	N/A
41.	• take appropriate steps to mitigate security risks so that the firm's overall security exposure is acceptable;	For more information on how you can mitigate security risks refer to Row 37 on "Security of your data and applications in the cloud".	N/A
42.	• consider data sensitivity and how the data are transmitted, stored and encrypted, where necessary.	The security of your data is of paramount importance to Google. 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 at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not	N/A

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (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	
43.	**Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR)**		
44.	A firm must comply with the DPA and the GDPR. Data protection requirements are separate from FCA Handbook requirements and each must be met separately.	Google will comply with its obligations under the DPA and GDPR applicable to it in the provision of the Services. In addition, Google makes commitments to protect your data, including regarding security, use, transfer, access and retention, in the Data Processing Amendment.	Representations and Warranties
45.	The DPA and GDPR are overseen and regulated by the Information Commissioner's Office (ICO). Firms should therefore follow the ICO's Guide to Data Protection and Guide to the GDPR, as well as other relevant guidance including that on cloud computing: https://ico.org.uk/media/for-organisations/documents/1540/cloud computing guidance for organisations.pdf	For more information on how Google Cloud can assist you in complying with data protection requirements see our GDPR resource center.	N/A
46.	Where relevant, firms should also consult ICO guidance on sending personal data outside the European Economic Area: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/	For more information on where your data is processed and stored refer to Row 38.	N/A
47.	**NIS Regulations**		
48.	Firms may also have to comply with the NIS Regulations 2018 where they meet the definition of a digital service provider (online search engines, online marketplaces and cloud computing services). These requirements are also separate from FCA Handbook requirements as well as data protection requirements.	Google will comply with all national laws and regulations applicable to it in the provisions of the Services.	Representations and Warranties

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
49.	Firms that are classed as relevant digital service providers under the NIS Regulations are also regulated by the ICO. Firms should therefore follow the ICO s Guide to NIS for more information on their obligations, including on registration requirements: https://ico.org.uk/for-organisations/the-guide-to-nis/	This is a customer consideration.	N/A
50.	**Effective access to data**		
51.	Specific regulatory requirements for some firms (e.g. SYSC 8.1.8R(9) for UCITS investment firms and Article 31(2)(i) MiFID Org Regulation for MiFID investment firms) require effective access to data related to the outsourced activities for regulated firms, their auditors, regulators and relevant competent authorities. The term data has a wide meaning. It includes but is not limited to firm, personal customer and transactional data, but also system and process data: for example, Human Resource vetting procedures or system audit trails and logs. A firm should:	Google recognizes that using our Services should not impair a regulated entities (or their supervisory authority's) ability to oversee and supervise compliance with applicable laws and regulations as well as a regulated entity's internal policies. We will provide regulated entities with the assistance they need to review our Services.	Enabling Customer Compliance
52.	• ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive;	Regulated entities may access their data on the services at any time.	Customer Information, Audit and Access
53.	• ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data;	Regulated entities may access their data on the services at any time. There is no restriction on the number of times a customer can access its own data.	Customer Information, Audit and Access
54.	• advise the service provider that the regulator will not enter into a non-disclosure agreement with the service provider but will treat any information disclosed in accordance with the confidentiality obligation set out in the Financial Services and Markets Act (FSMA), sections 348 to 349;	Google understands that it may not be possible for supervisory authorities to enter into non-disclosure agreements where they are subject to confidentiality obligations under the law.	N/A
55.	• ensure that, where a firm cannot disclose data for any reason, the contract enables the regulator or the firm's auditor to contact the service provider directly;	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Regulator Information, Audit and Access
56.	• ensure that data are not stored in jurisdictions that may inhibit effective access to data for UK regulators. Considerations should include the wider political and security stability of the jurisdiction; the law in force in the jurisdiction in question (including data protection); and the international obligations of the jurisdiction. This should include consideration of the law enforcement provisions within a jurisdiction.	Google grants audit, access and information rights to supervisory authorities and their appointees. These rights apply regardless of the service location.For more information on the location of Google's facilities and where individual Google Workspace services can be deployed, refer to Row 38.	Regulator Information, Audit and Access
57.	**Access to business premises**		
58.	SYSC 8.1.8R(9) requires UCITS investment firms to have "effective access to data related to the outsourced activities, as well as to the business premises of the service provider".	Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and supervisory	Regulator Information, Audit and Access Customer Information, Audit and Access

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Article 31(2)(i) MiFID Org Regulation requires that "the investment firm, its auditors and the relevant competent authorities have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with this article, and the competent authorities are able to exercise those rights of access"	authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	
59.	We regard 'business premises' as a broad term, encompassing a range of premises. This may include head offices, operations centres, but does not necessarily include data centres.	Refer to Row 58.	N/A
60.	For firms where these requirements apply as rules or directly applicable provisions, their contracts must allow for access to business premises. The focus should therefore be on which business premises are relevant for the exercise of effective oversight; this does not necessarily require access to all business premises. For example, service providers may, for legitimate security reasons, limit access to some sites - such as data centres.	Refer to Row 58.	N/A
61.	Firms should also be aware of specific requirements in other relevant legislation. For example, Article 274 of the Solvency II Regulation requires the insurance or reinsurance undertaking to have "effective access to all information relating to the outsourced functions and activities, including carrying out on-site inspections of the business premises of the service provider".	Refer to Row 58.	N/A
62.	Particular considerations include:		
63.	**Firm and auditor access**		
64.	• A firm should be able to request an onsite visit to the relevant business premises, in accordance with applicable legal and regulatory requirements. This right should not be restricted;	Nothing in our contract is intended to restrict a regulated entity's ability to monitor or audit our services effectively. In particular, although we will make a lot of information and tools available to help regulated entities and their supervisory authorities review our Services, our contract does not contain pre-defined steps before regulated entities or supervisory authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services. For more information on the audit, access and information rights granted to regulated entities refer to Row 58.	Enabling Customer Compliance
65.	• A firm can provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation;	Reasonable notice enables Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it does not create undue risk to your environment or that of any other Google customer. Google recognizes that in some cases extended notice is not possible. In these cases we will work with the auditing party to address their needs.	Arrangements

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
66.	• A firm may elect its auditor to undertake the visit. Note that this must be the firm's auditor and not an auditor appointed by the outsourcing provider	Google facilitates audits by regulated entities and their appointed auditors. For more information on the audit, access and information rights, refer to Row 58.	N/A
67.	• The scope of the firm and/or auditor visit can be limited to those services that the firm and the entities in the firm's group are using, as required by applicable legal and regulatory requirements.	The regulated entity is best placed to decide what audit scope is right for their organization. Our contract does not limit regulated entities to a pre-defined scope.	Customer Information, Audit and Access
68.	**Regulator access**		
69.	• A regulator visit to an outsource provider's business premises will only take place if the regulator deems it necessary and required under applicable legal and regulatory requirements. Firms should not stipulate further conditions beyond this.	Nothing in our contract is intended to restrict the supervisory authority's ability to monitor or audit our services effectively.	Enabling Customer Compliance
70.	• The outsource provider should commit to cooperate with the reasonable requests of the regulator during such a visit.	Google will fully cooperate with supervisory authorities exercising their audit, information and access rights.	Enabling Customer Compliance
71.	• The regulator can commit to visits occurring during business hours and at a time specified by the outsourcing provider or with reasonable notice, except in an emergency or crisis situation.	For more information on the timing of audits refer to Row 65.	N/A
72.	• There can be no restrictions regarding employees who attend from the regulator. However, regulators can and will provide relevant information about individuals who will attend.	Google does not place restrictions on who may attend an audit from the supervisory authority.	Regulator Information, Audit and Access
73.	• During the visit, the regulator should be permitted to view the provision of services to the regulated firm or any affiliate within the group, as required under applicable financial services legislation. The regulator can commit to minimising, disruption to outsourcing providers operations.	It is extremely important to Google that what we do with one customer should not put any other customers at risk. This applies when you perform an audit. It also applies when any other customer performs an audit. When a supervisory authority performs an audit we will work with them to minimize the disruption to our other customers. Just as we will work with another auditing customer to minimize the disruption to the regulated entity. In particular, we will be careful to comply with our security commitments at all times.	Arrangements
74.	**Relationship between service providers**		
75.	Outsourcing supply chains are often complex. If the regulated firm does not directly contract with the outsource provider, it should review sub-contracting arrangements relevant to the provision of the regulated activity to determine whether these enable the regulated firm to continue to comply with its regulatory requirements. Firms should consider, for example, security requirements and	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Google will remain accountable to you for the performance of all subcontracted obligations. To enable regulated entities to retain oversight of any subcontracting and provide	Google Subcontractors

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	effective access to data and business premises. The regulated firm must be able to comply with these regulatory requirements even if it does not directly contract with the outsource provider.	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 will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights).	
76.	The Contracts (Rights of Third Parties) Act 1999 may be relevant to these considerations.	This is a customer consideration.	N/A
77.	The regulated firm should consider how service providers work together. For example, will the firm or one service provider take the lead systems integration role?	This is a customer consideration.	N/A
78.	Firms should consider how easily a service provider's services will interface with a firm's internal systems or other third-party systems (such as agency banking arrangements for payments).	There are a number of ways to integrate our services with your systems. Integration There are a number of ways to integrate our services with your systems. • Google Workspace Marketplace API allows you to access a repository of Google Workspace APIs in a centralised location for easy integration. • Google Workspace also enables you to integrate with reliable third-party business solutions. More information is available on our Partner Integration page.	N/A
79.	**Change management**		
80.	Risks can be introduced when changes are made to processes and procedures even where these are well established. We expect firms to have in place a comprehensive change management process, but particular note should be taken of the following points:	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 control changes to your use of the services. Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time.	Changes to Services

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	
81.	• establishing what provision has been made for making future changes to technology service provision;	Refer to Row 80.	N/A
82.	• establishing how the testing of changes will be carried out.	Refer to Row 80.	N/A
83.	**Continuity and business planning**		
84.	A firm should have in place appropriate arrangements to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption of the outsourced services. Firms should:	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. More information on the reliability of the Services is available on our Google Cloud Help page.	Business Continuity and Disaster Recovery
85.	• consider the likelihood and impact of an unexpected disruption to the continuity of its operations;	Refer to Row 84.	N/A
86.	• document its strategy for maintaining continuity of its operations, including recovery from an event, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy;	Refer to Row 84.	N/A
87.	• regularly update and test arrangements to ensure their effectiveness;	Refer to Row 84.	N/A
88.	• put in place arrangements to ensure the regulator has access to data in the event of insolvency or other disruption.	For more information on the regulator's data access rights refer to Row 55. None of these commitments are disapplied on Google's insolvency. For more information on how Google supports regulated entities through resolution, refer to Row 91.	N/A
89.	**Resolution (where applicable)**		

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
90.	Any services should be organised in such a way that they do not become a barrier to the resolution or orderly wind-down of a firm, or create additional complexity in a resolution.	This is a customer consideration.	N/A
91.	For firms where stabilisation powers will, or may, be applied, this will mean that the outsourcing provider and any subcontractor should agree that neither the entry into resolution nor a subsequent change in control arising from the firm's entry into resolution shall constitute a termination event. The outsourcing provider should also agree not to delete, revoke, alter or change any data and to continue to provide services to the firm (or such other entity as necessary) for an appropriate transitional period following the resolution.	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
92.	For firms where insolvency procedures will be used, services should be set up in such a way that supports the rapid return of the firms' deposits or client assets. For example, services should be organised in such a way that would not impede the production of a Single Customer View (SCV) file in a Bank Insolvency Procedure (BIP) or the production of accurate data around client assets in a Special Administration Regime (SAR).	This is a customer consideration.	N/A
93.	**Exit plan**		
94.	Firms need to ensure that they are able to exit outsourcing plans, should they wish to, without undue disruption to their provision of services, or their compliance with the regulatory regime. Firms should:	Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to the regulated entity or another service provider). 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. Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our Google Account help page. In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. 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 Term Transition Assistance
95.	• have exit plans and termination arrangements that are understood, documented and fully tested;	Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with the law.	Term and Termination

FCA - FG 16/5

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency.	
96.	• know how it would transition to an alternative service provider and maintain business continuity;	For more information on the substitutability of our services refer to Row 94.	N/A
97.	• have a specific obligation put on the outsourcing provider to cooperate fully with both the firm and any new outsource provider(s) to ensure there is a smooth transition;	For more information on how Google may assist on exit refer to Row 94.	N/A
98.	• know how it would remove data from the service provider's systems on exit;	For more information on transferring data on exit, refer to Row 94.	N/A
99.	• monitor concentration risk and consider what action it would take if the outsource provider failed.	This is a customer consideration	N/A