FCA - SYSC 8

Google Workspace Mapping

This document is designed to help firms supervised by the Financial Conduct Authority ("**regulated entity**") to consider SYSC 8.1 General Outsourcing Requirements (the "**framework**") in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: SYSC 8.1.1 to SYSC 8.1.9. 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.	8.1.1(1)	A common platform must: when relying on a third party for the performance of operational functions which are critical for the performance of *regulated activities*, *listed activities* or *ancillary services* (in this chapter "relevant services and activities") on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk; and	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 on Google's security infrastructure refer to Row 31.	N/A
2.	8.1.1(2)	not undertake the *outsourcing* of important operational functions in such a way as to impair materially:		
3.	8.1.1(2)(a)	the quality of its internal control; and	You can provide Google instructions about your data and Google will comply with those instructions. Regulated entities can use the following functionality to control the Services: • Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources. In addition, refer to Row 7 for more information on how you can monitor Google's performance of the Services.	Google's Compliance with Instructions (Data Processing Amendment) Instructions
4.	8.1.1(2)(b)	the ability of the *FCA* to monitor the *firm's* compliance with all obligations under the *regulatory system* and, if different, of a *competent authority* to monitor the *firm's* compliance with all obligations under *MiFID*. [**Note:** article 16(5) first paragraph of *MiFID*]	Google will fully cooperate with supervisory authorities exercising their audit, information and access rights. For more information on the audit, information and access rights granted to supervisory authorities refer to Row 30.	Enabling Customer Compliance
5.	8.1.1A	Other *firms* should take account of the outsourcing *rule* (*SYSC 8.1.1 R*) as if it were *guidance* (and as if should appeared in that *rule* instead of must) as explained in *SYSC 1 Annex 1* 3.3R(1).	This is a customer consideration.	N/A
6.	8.1.2	The application of *SYSC 8.1* to relevant services and activities (see *SYSC 8.1.1 R (1)*) is limited by *SYSC 1 Annex 1 (Part 2)* (Application of the common platform requirements).	This is a customer consideration.	N/A
7.	8.1.3	*SYSC 4.1.1 R* requires a *firm* to have effective processes to identify, manage, monitor and report risks and internal control mechanisms. Except in relation to those functions described in *SYSC 8.1.5R* and (for a *common platform firm* in article 30(2) of the *MiFID Org Regulation*), where a *firm* relies on a third party for the performance of operational functions which are not critical or important for the performance of relevant services and activities (see *SYSC 8.1.1 R (1)*) on a continuous and satisfactory basis,	Monitoring the service You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example:	Ongoing Performance Monitoring

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		it should take into account, in a manner that is proportionate given the nature, scale and complexity of the *outsourcing*, the *rules* in this section in complying with that requirement.	• 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). Incident notification For more information on Google's incident notification process refer to Row 27	N/A
8.	8.1.4	For the purposes of this chapter an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a *firm* other than a (*common platform firm*) with the conditions and obligations of its *authorisation* or its other obligations under the *regulatory system*, or its financial performance, or the soundness or the continuity of its relevant services and activities.	This is a customer consideration.	N/A
9.	8.1.5	For a *UCITS investment firm* and without prejudice to the status of any other function, the following functions will not be considered as critical or important for the purposes of this chapter:	This is a customer consideration.	N/A
10.	8.1.5(1)	the provision to the *firm* of advisory services, and other services which do not form part of the relevant services and activities of the *firm*, including the provision of legal advice to the *firm*, the training of personnel of the *firm*, billing services and the security of the *firm's* premises and personnel;	This is a customer consideration.	N/A
11.	8.1.5(2)	the purchase of standardised services, including market information services and the provision of price feeds;	This is a customer consideration.	N/A
12.	8.1.5(3)	the recording and retention of relevant telephone conversations or electronic communications subject to SYSC 10A.	This is a customer consideration.	N/A
13.	8.1.5A	Other *firms* should take account of the critical functions *rules* (*SYSC 8.1.4 R* and *SYSC 8.1.5 R*) as if they were *guidance* (and as if should appeared in those *rules* instead of must) as explained in *SYSC 1 Annex 1* 3.3R(1).	This is a customer consideration.	N/A

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
14.	8.1.6	If a *firm* (other than a *common platform firm*) *outsources* critical or important operational functions or any relevant services and activities, it remains fully responsible for discharging all of its obligations under the *regulatory system* and must comply, in particular, with the following conditions:	This is a customer consideration.	N/A
15.	8.1.6(1)	the *outsourcing* must not result in the delegation by *senior personnel* of their responsibility;	This is a customer consideration.	N/A
16.	8.1.6(2)	the relationship and obligations of the *firm* towards its *clients* under the *regulatory system* must not be altered;	This is a customer consideration.	N/A
17.	8.1.6(3)	the conditions with which the *firm* must comply in order to be *authorised*, and to remain so, must not be undermined;	This is a customer consideration.	N/A
18.	8.1.6(4)	none of the other conditions subject to which the *firm's authorisation* was granted must be removed or modified.	This is a customer consideration.	N/A
19.	8.1.6A	A *UCITS investment firm* should take account of the provisions that apply to a *common platform firm* in relation to its *MiFID business* in accordance with *SYSC 8.1.-2G*.	This is a customer consideration.	N/A
20.	8.1.7	A *UCITS investment firm* must exercise due skill and care and diligence when entering into, managing or terminating any arrangement for the *outsourcing* to a service provider of critical or important operational functions or of any relevant services and activities.	This is a customer consideration.	N/A
21.	8.1.8	A *UCITS investment firm* must in particular take the necessary steps to ensure that the following conditions are satisfied:	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 information for each of the areas you need to consider in the rows that follow.	N/A
22.	8.1.8(1)	the service provider must have the ability, capacity, and any *authorisation* required by law to perform the *outsourced* functions, services or activities reliably and professionally;	Ability • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Workspace Customer page. Capacity • Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science,	N/A

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. • Information about Google Cloud's leadership team is available on our Media Resources page. • You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. Authorisation Google will comply with all laws and regulations applicable to it in the provision of the Services	
23.	8.1.8(2)	the service provider must carry out the *outsourced* services effectively, and to this end the *firm* must establish methods for assessing the standard of performance of the service provider;	The SLAs provide measurable performance standards and remedies for the services and are available on our Google Workspace Service Level Agreements page.	Services
24.	8.1.8(3)	the service provider must properly supervise the carrying out of the *outsourced* functions, and adequately manage the risks associated with the *outsourcing*;	Supervision by Google senior executives Google executive management reviews and approves all information security policies and sets applicable commitment and direction to achieve the agreed upon Information Security goals. Google's senior executive is also responsible for approving Google's ISO27001 ISMS and other key compliance frameworks. Google's security management team, with support from our executive team, maintains a robust security infrastructure. Management evaluates, directs and supervises security at an organisational and product level and ensures security is embedded at all levels of our products. Monitoring and risk management by Google personnel Google employs security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure and implementing Google's security policies. Google's dedicated security team actively scans for security risks using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews. Incident response For more information on Google's incident notification process refer to Row 27.	N/A

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
25.	8.1.8(4)	appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements;	This is a customer consideration.	N/A
26.	8.1.8(5)	the *firm* must retain the necessary expertise to supervise the *outsourced* functions effectively and to manage the risks associated with the *outsourcing*, and must supervise those functions and manage those risks;	Regulated entity expertise This is a customer consideration. Regulated entity supervision For more information on how a regulated entity may supervise and control outsourced functions refer to Rows 3 and 7.	N/A
27.	8.1.8(6)	the service provider must disclose to the *firm* any development that may have a material impact on its ability to carry out the *outsourced* functions effectively and in compliance with applicable laws and regulatory requirements;	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. For more information on how a regulated entity may monitor Google's performance of the Services, refer to Row 7.	Significant Developments Data Incidents (Data Processing Amendment) N/A
28.	8.1.8(7)	the *firm* must be able to terminate the arrangement for the *outsourcing* where necessary without detriment to the continuity and quality of its provision of services to *clients*;	Cease use of service If you wish to stop using our services you may do so at any time. Transition Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to 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.	Ceasing Services Use Transition Term Data Export (Data Processing Amendment)

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.	
29.	8.1.8(8)	the service provider must co-operate with the *FCA* and any other relevant *competent authority* in connection with the *outsourced* activities;	Google will fully cooperate with supervisory authorities exercising their audit, information and access rights.	Enabling Customer Compliance
30.	8.1.8(9)	the *firm*, its auditors, the *FCA* and any other relevant *competent authority* must have effective access to data related to the *outsourced* activities, as well as to the business premises of the service provider; and the *FCA* and any other relevant *competent authority* must be able to exercise those rights of access;	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 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
31.	8.1.8(10)	the service provider must protect any confidential information relating to the *firm* and its *clients*;	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. 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 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	Confidentiality Data Security; Security Measures (Data Processing Amendment)

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. 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 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 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	
32.	8.1.8(11) the *firm* and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup	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.	Business Continuity and Disaster Recovery

FCA - SYSC 8

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		facilities where that is necessary having regard to the function, service or activity that has been *outsourced*.	More information on the reliability of the Services is available on our Google Cloud Help page.	
33.	8.1.9	A *UCITS investment firm* must ensure that the respective rights and obligations of the *firm* and of the service provider are clearly allocated and set out in a written agreement.	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
34.	8.1.10	If a *UCITS investment firm* and the service provider are members of the same *group*, the *firm* may, for the purpose of complying with *SYSC 8.1.7 R* to *SYSC 8.1.11 R* and *SYSC 8.2* and *SYSC 8.3*, take into account the extent to which the *UCITS investment firm controls* the service provider or has the ability to influence its actions.	This is a customer consideration.	N/A
35.	8.1.11	A *firm* (other than a *common platform firm*) must make available on request to the *FCA* and any other relevant *competent authority* all information necessary to enable the *FCA* and any other relevant *competent authority* to supervise the compliance of the performance of the *outsourced* activities with the requirements of the *regulatory system*.	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 Customer Information, Audit and Access