ESMA Guidelines on Outsourcing to Cloud Service Providers

Google Cloud Mapping

This document is designed to help firms within the scope of the European Securities and Markets Authority's mandate ("**regulated entity**") to consider the Guidelines on outsourcing to cloud service providers ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Guideline 3 - Key contractual elements, Guideline 4 - Information security, Guideline 5 - Exit strategies, Guideline 6 - Access and audit rights and Guideline 7 - Sub-outsourcing . 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
Guideline 3. Key contractual elements			
1.	26. The respective rights and obligations of a firm and its CSP should be clearly 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
2.	27. The written agreement should expressly allow the possibility for the firm to terminate it, where necessary.	You can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority.	Termination for Convenience
3.	28. In case of outsourcing of critical or important functions, the written agreement should include at least:		
4.	a) a clear description of the outsourced function;	The GCP services are described on our services summary page.	Definitions
5.	b) the start date and end date, where applicable, of the agreement and the notice periods for the CSP and for the firm;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
6.	c) the governing law of the agreement and, if any, the choice of jurisdiction;	Refer to your Google Cloud Financial Services Contract.	Governing Law
7.	d) the firm's and the CSP's financial obligations;	Refer to your Google Cloud Financial Services Contract.	Payment Terms
8.	e) whether sub-outsourcing is permitted, and, if so, under which conditions, having regard to Guideline 7;	For more information on sub-outsourcing refer to Rows 58 to 65.	N/A
9.	f) the location(s) (namely regions or countries) where the outsourced function will be provided and where data will be processed and stored, and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s);	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 GCP 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.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

#	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. Conditions Google provides you with choices about where to store your data - including a choice to store your data in Europe. 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 European customers on Google Cloud Whitepaper. In addition, Google provides commitments to enable the lawful transfer of personal data to a third country in accordance with European data protection law.	Data Location (Service Specific Terms) Data Transfers (Cloud Data Processing Addendum)
10.	g) provisions regarding information security and protection of personal data, having regard to Guideline 4;	For more information on information security and protection of personal data, refer to Rows 19 to 28.	N/A
11.	h) the right for the firm to monitor the CSP's performance under the cloud outsourcing arrangement on a regular basis, having regard to Guideline 6;	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 GCP. • 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	Ongoing Performance Monitoring

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
12.	i) the agreed service levels, which should include, quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;	The SLAs are available on our Google Cloud Platform Service Level Agreements page.	Services
13.	j) the reporting obligations of the CSP to the firm and, as appropriate, the obligations to submit reports relevant for the firm's security function and key functions, such as reports prepared by the internal audit function of the CSP;	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.	Significant Developments
14.	k) provisions regarding the management of incidents by the CSP, including the obligation for the CSP to report to the firm without undue delay incidents that have affected the operation of the firm's contracted service;	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)
15.	l) whether the CSP should take 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.	Insurance
16.	m) the requirements for the CSP to implement and test business continuity and disaster recovery plans;	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. 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
17.	n) the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by the firm or the competent authorities the right to access ('access rights') and to inspect ('audit rights') the relevant information, premises, systems and devices of the CSP to the extent necessary to monitor the CSP's performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements, having regard to Guideline 6;	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

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
18.	o) provisions to ensure that the data that the CSP processes or stores on behalf of the firm can be accessed, recovered and returned to the firm as needed, having regard to Guideline 5.	Regulated entities may access their data on the services at any time. For more information on data export , refer to Row 32.	N/A
Guideline 4. Information security			
19.	29. A firm should set information security requirements in its internal policies and procedures and within the cloud outsourcing written agreement and monitor compliance with these requirements on an ongoing basis, including to protect confidential, personal or otherwise sensitive data. These requirements should be proportionate to the nature, scale and complexity of the function that the firm outsources to the CSP and the risks inherent to this function.	The security 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. Refer to Row 28. (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	Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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	
20.	30. For that purpose, in case of outsourcing of critical or important functions, and without prejudice to the applicable requirements under GDPR, a firm, applying a risk-based approach, should at least:		
21.	p) *information security organisation*: ensure that there is a clear allocation of information security roles and responsibilities between the firm and the CSP, including in relation to threat detection, incident management and patch management, and ensure that the CSP is effectively able to fulfil its roles and responsibilities	For more information on the allocation of information security roles and responsibilities, refer to Row 19.	N/A
22.	q) *identity and access management*: ensure that strong authentication mechanisms (for example multi-factor authentication) and access	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service.	N/A

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		controls are in place with a view to prevent unauthorised access to the firm's data and back-end cloud resources;	- Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. - Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. - Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: - 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). - Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	
23.	r)	*encryption and key management*: ensure that relevant encryption technologies are used, where necessary, for data in transit, data in memory, data at rest and data back-ups, in combination with appropriate key management solutions to limit the risk of non-authorised access to the encryption keys; in particular, the firm should consider state-of-the-art technology and processes when selecting its key management solution;	For more information about encryption at rest and encryption in transit, refer to Row 19. In addition, you can choose to use these encryption and key management tools provided by Google: - Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. - Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. - Customer-managed encryption keys for Cloud SQL and GKE persistent disks. - Cloud External Key Manager (beta) lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. - Key Access Justification (alpha) works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set.	
24.	s) *operations and network security*: consider appropriate levels of network availability, network segregation(for example tenant isolation in the shared environment of the cloud, operational separation as regards the web, application logic, operating system, network, Data Base Management System (DBMS) and storage layers) and processing environments (for example test, User Acceptance Testing, development, production)	Availability The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. In addition, you can choose to use these networking tools provided by Google: - Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications. - Dedicated Interconnect is a high-performance option providing direct physical connections between your on-premises network and Google's network. Resource isolation To keep data private and secure, Google logically isolates each customer's data from that of other customers. Refer to Row 19 for more information on Google's security.	Services Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
25.	t) *application programming interfaces (API)*: consider mechanisms for the integration of the cloud services with the systems of the firm to ensure security of APIs (for example establishing and maintaining information	There are a number of ways to integrate our services with your systems and to perform effective access management.	N/A

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		security policies and procedures for APIs across multiple system interfaces, jurisdictions, and business functions to prevent unauthorised disclosure, modification or destruction of data);	**Integration** • Cloud Console allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage. • Cloud APIs allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language. **Access management** • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. • Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.	
26.	u)	*business continuity and disaster recovery*: ensure that effective business continuity and disaster recovery controls are in place (for example by setting minimum capacity requirements, selecting hosting options that are geographically spread, with the capability to switch from one to the other, or requesting and reviewing documentation showing the transport route of the firm's data among the CSP's systems, as well as considering the possibility to replicate machine images to an independent storage location, which is sufficiently isolated from the network or taken offline);	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. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. In particular, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired resilience for your applications.	Business Continuity and Disaster Recovery

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
27.	v) *data location*: adopt a risk-based approach to data storage and data processing location(s) (namely regions or countries);	This is a customer consideration. For more information on data location and the choices regulated entities have refer to Row 9.	N/A
28.	w) *compliance & monitoring*: verify that the CSP complies with internationally recognised information security standards and has implemented appropriate information security controls (for example by requesting the CSP to provide evidence that it conducts relevant information security reviews and by performing regular assessments and tests on the CSP's information security arrangements).	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.	Certifications and Audit Reports
Guideline 5. Exit strategies			
29.	31. In case of outsourcing of critical or important functions, a firm should ensure that it is able to exit the cloud outsourcing arrangement without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with its obligations under the applicable legislation, as well as the confidentiality, integrity and availability of its data. For that purpose, a firm should:	Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law, or where directed by the supervisory authority. 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.	Termination for Convenience Transition Term
30.	x) develop exit plans that are comprehensive, documented and sufficiently tested. These plans should be updated as needed, including in case of changes in the outsourced function;	This is a customer consideration.	N/A
31.	y) identify alternative solutions and develop transition plans to remove the outsourced function and data from the CSP and, where applicable, any sub-outsourcer, and transfer them to the alternative CSP indicated by the firm or directly back to the firm. These solutions should be defined with regard to the challenges that may arise from the location of the	This is a customer consideration.	N/A

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		data, taking the necessary measures to ensure business continuity during the transition phase;		
32.	z)	ensure that the cloud outsourcing written agreement includes an obligation for the CSP to support the orderly transfer of the outsourced function, and the related processing of data, from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy. The obligation to support the orderly transfer of the outsourced function, and the related treatment of data, should include where relevant the secure deletion of the data from the systems of the CSP and any sub-outsourcer.	Support Google will enable you to access and export your data throughout the duration of our contract and during the additional 12 month transition period. 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. 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. Deletion On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. For more information about deletion refer to our Deletion on Google Cloud Platform whitepaper.	Data Export (Cloud Data Processing Addendum) Transition Assistance Deletion on Termination (Cloud Data Processing Addendum)
33.	32. When developing the exit plans and solutions referred to in points (a) and (b) above ('exit strategy'), the firm should consider the following:			
34.	aa)	define the objectives of the exit strategy;	This is a customer consideration.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
35.	bb) define the trigger events that could activate the exit strategy. These should include at least the termination of the cloud outsourcing arrangement at the initiative of the firm or the CSP and the failure or other serious discontinuation of the business activity of the CSP;	This is a customer consideration.	N/A
36.	cc) perform a business impact analysis that is commensurate to the function outsourced to identify what human and other resources would be required to implement the exit strategy;	This is a customer consideration.	N/A
37.	dd) assign roles and responsibilities to manage the exit strategy;	This is a customer consideration.	N/A
38.	ee) test the appropriateness of the exit strategy, using a risk-based approach, (for example, by carrying out an analysis of the potential costs, impact, resources and timing implications of transferring an outsourced service to an alternative provider);	This is a customer consideration.	N/A
39.	ff) define success criteria of the transition.	This is a customer consideration.	N/A
40.	33. A firm should include indicators of the trigger events of the exit strategy in its ongoing monitoring and oversight of the services provided by the CSP under the cloud outsourcing arrangement.	This is a customer consideration.	N/A
Guideline 6. Access and Audit Rights			
41.	34. A firm should ensure that the cloud outsourcing written agreement does not limit the firm's and competent authority's effective exercise of the access and audit rights and oversight options on the CSP.	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. In particular, although we will make a lot of information and tools available to help regulated entities 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.	Enabling Customer Compliance
42.	35. A firm should ensure that the exercise of the access and audit rights (for example, the audit frequency and the areas and services to be audited) takes into consideration whether the outsourcing is related to a critical or important function, as well as the	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

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	nature and extent of the risks and impact arising from the cloud outsourcing arrangement on the firm.		
43.	36. In case the exercise of the access or audit rights, or the use of certain audit techniques create a risk for the environment of the CSP and/or another CSP's client (for example by impacting service levels, confidentiality, integrity and availability of data), the CSP should provide a clear rationale to the firm as to why this would create a risk and the CSP should agree with the firm on alternative ways to achieve a similar result (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the CSP).	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 regulated entity 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
44.	37. Without prejudice to their final responsibility regarding cloud outsourcing arrangements, in order to use audit resources more efficiently and decrease the organisational burden on the CSP and its clients, firms may use:		
45.	gg) third-party certifications and external or internal audit reports made available by the CSP;	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.	Certifications and Audit Reports
46.	hh) pooled audits performed jointly with other clients of the same CSP or pooled audits performed by a third-party auditor appointed by multiple clients of the same CSP.	Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
47.	38. In case of outsourcing of critical or important functions, a firm should assess whether the third-party certifications and external or internal audit reports referred to in paragraph 37(a) are adequate and sufficient to comply with its obligations under the applicable legislation and should aim at not solely relying on these certifications and reports over time.	This is a customer consideration.	N/A
48.	39. In case of outsourcing of critical or important functions, a firm should make use of the third-party certifications and external or internal audit reports referred to in paragraph 37(a) only if it:		
49.	ii) is satisfied that the scope of the certifications or the audit reports covers the CSP's key systems (for example processes, applications, infrastructure, data centres), the key controls identified by the firm and the compliance with the relevant applicable legislation;	Refer to Row 45. 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
50.	jj) thoroughly assesses the content of the certifications or audit reports on a regular basis and verify that the certifications or reports are not obsolete;	Refer to Row 45. You can review Google's current certifications and audit reports at any time.	Certifications and Audit Reports
51.	kk) ensures that the CSP's key systems and controls are covered in future versions of the certifications or audit reports;	Refer to Row 45. 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
52.	ll) is satisfied with the certifying or auditing party (for example with regard to its qualifications, expertise, re-performance/verification of the evidence in the underlying audit file as well as rotation of the certifying or auditing company);	Refer to Row 45. 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
53.	mm) is satisfied that the certifications are issued and that the audits are performed according to appropriate standards and include a test of the effectiveness of the key controls in place;	Refer to Row 45. Audits include testing of operational effectiveness of key controls in place.	Certifications and Audit Reports

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
54.	nn) has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls of the CSP; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective;	To ensure that they remain an effective tool, if a key system or control for a Service is not covered by Google's certifications or audit reports for that service, regulated entities can request an expansion of the scope.	Certifications and Audit Reports
55.	oo) retains the contractual right to perform individual on-site audits at its discretion with regard to the outsourced function.	Regulated entities always retain the right to conduct an audit. The contract does not contain pre-defined steps before regulated entities 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.	Customer Information, Audit and Access
56.	40. A firm should ensure that, before an on-site visit, including by a third party appointed by the firm (for example an auditor), prior notice within a reasonable time period is provided to the CSP, unless an early prior notification is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective. Such notice should include the location, purpose of the visit and the personnel that will participate to the visit.	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
57.	41. Considering that cloud services present a high level of technical complexity and raise specific jurisdictional challenges, the staff performing the audit –being the internal auditors of the firm or auditors acting on its behalf –should have the right skills and knowledge to properly assess the relevant cloud services and perform effective and relevant audit. This should also apply to the firms' staff reviewing the certifications or audit reports provided by the CSP.	This is a customer consideration.	N/A
Guideline 7. Sub-outsourcing			
58.	42. If sub-outsourcing of critical or important functions (or material parts thereof) is permitted, the cloud outsourcing written agreement between the firm and the CSP should:		
59.	pp) specify any part or aspect of the outsourced function that are excluded from potential sub-outsourcing;	Google recognizes that regulated entities need to consider the risks associated with sub-outsourcing. 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 sub-outsource. Given the one-to-many nature	Subcontracting

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		of our service, if we agreed with one customer that we would not sub-outsource, we would potentially be denying all our customers the benefit motivating the sub-outsourcing. To ensure regulated entities retain oversight of any sub-outsourcing, Google will comply with clear conditions designed to provide transparency and choice. Refer to Row 60.	
60.	qq) indicate the conditions to be complied with in case of sub-outsourcing;	To enable regulated entities to retain oversight of any sub-outsourcing 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 will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights, and security requirements).	Google Subcontractors
61.	rr) specify that the CSP remains accountable and is obliged to oversee those services that it has sub-outsourced to ensure that all contractual obligations between the CSP and the firm are continuously met;	Refer to Row 60.	Google Subcontractors
62.	ss) include an obligation for the CSP to notify the firm of any intended sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the firm. The notification period set in the written agreement should allow the firm sufficient time at least to carry out a risk assessment of the proposed sub-outsourcing or material changes thereof and to object to or explicitly approve them, as indicated in point (e) below;	You need enough time from being informed of a subcontractor change to perform a meaningful risk assessment before the change comes into effect. To ensure you have the time you need, Google provides advance notice before we engage a new subcontractor or change the function of an existing subcontractor.	Google Subcontractors
63.	tt) ensure that the firm has the right to object to the intended sub-outsourcing, or material changes thereof, or that explicit approval is required before the proposed sub-outsourcing or material changes come into effect;	Regulated entities have the choice to terminate our contract if they think that a subcontractor change materially increases their risk. Refer to Row 64.	Google Subcontractors

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
64.	uu) ensure that the firm has the contractual right to terminate the cloud outsourcing arrangement with the CSP in case it objects to the proposed sub-outsourcing or material changes thereof and in case of undue sub-outsourcing(for example where the CSP proceeds with the sub-outsourcing without notifying the firm or it seriously infringes the conditions of the sub-outsourcing specified in the outsourcing agreement).	Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors
65.	43. The firm should ensure that the CSP appropriately oversees the sub-outsourcer.	Refer to Row 60.	N/A