FINMA - Circular 2018/3

Google Cloud Mapping

This document is designed to help banks, securities dealers and insurance companies supervised by the Swiss Financial Market Supervisory Authority FINMA (“**regulated entity**”) to consider FINMA Circular 2018/3 “Outsourcing - banks and insurers” (the “**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on section V, “Requirements for outsourcing companies”, which covers the following requirements of the framework: A. Inventory of outsourced functions, B. Selection, instruction and monitoring of the service provider, C. Outsourcing within a group or conglomerate, D. Responsibility, E. Security, F. Audit and supervision, G. Outsourcing to another country and H. Agreement. 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
A. Inventory of outsourced functions				
1	14.	An inventory of outsourced functions must be drawn up and kept up to date at all times. It must contain a description of the outsourced function and indicate the service provider (including subcontractors), the service recipient and the unit responsible within the outsourcing company (see Margin no. 20).	Inventory This is a customer consideration. Subcontractors Google will provide information about Google Subcontractors, refer to Row 22 for more information on subcontractors.	N/A N/A
2	15.	Insurance companies keep this inventory in conjunction with business plan form J.	This is a customer consideration.	N/A
3	15.1	Financial institutions under Margin nos. 6.1 and 6.2 and securities firms keep this inventory within the context of their organisational principles (Art. 17 para. 3 FinIO).	This is a customer consideration.	N/A
B. Selection, instruction and monitoring of the service provider				
4	16.	The service specifications must be agreed in line with the aims of the outsourcing and documented before the agreement is signed. This includes conducting a risk analysis that takes account of the main economic and operational considerations as well as the associated risks and opportunities.	Service specification The GCP services are described on our services summary page. Risk analysis From an operational perspective, GCP is controlled by the customer. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Customers can configure GCP to avoid undue operational risk. To assist with your risk assessment more information about Google is provided in Row 5 and information on Google’s security practices are provided in Row 13.	Definitions N/A
5	17.	The service provider must be chosen with due regard to, and subject to checks of, its professional capabilities as well as its financial and human resources. Where multiple functions are outsourced to the same service provider, the concentration of risk must be taken into account.	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 below. Professional Capabilities	N/A

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Qualifications and competencies: 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. • Customer references: Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. • Information about Google Cloud's service delivery capability and effectiveness is available on our Choosing Google Cloud page. Financial and human resources • You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page. • Principals: Information about Google Cloud's leadership team is available on our Media Resources page. Concentration risk Refer to Row 6 for more information on the substitutability of our services.	

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
6	18. Furthermore, the eventuality of a change of service provider and the possible consequences of such a change must be considered when deciding to outsource and selecting the service provider. The service provider must offer a guarantee of permanent service provision. Provision must be made for insourcing the outsourced function or transferring it to another service provider in an orderly manner.	Change of service provider/insourcing 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 during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. 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 Service.	Transition Term Data Export (Cloud Data Processing Addendum) Transition Assistance

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
7	18.1 Provision must be made for insourcing the outsourced function or transferring it to another service provider in an orderly manner.	See row above.	N/A
8	19. The duties of the company and the service provider must be contractually agreed and delimited, in particular with regard to interfaces and responsibilities.	The rights and responsibilities of the parties (and the interfaces between them) are set out in the Google Cloud Financial Services Contract.	N/A

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
9	20. The outsourced function must be integrated into the company's internal control system. The main risks associated with the outsourcing must be systematically identified, monitored, quantified and controlled. A unit within the company must be named as responsible for monitoring and controlling the service provider. The latter's services must be monitored and assessed on an ongoing basis so that any necessary measures can be taken promptly.	Integration There are a number of ways to integrate our services with your systems. • 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. Monitoring 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 number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Incident response 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.	N/A Ongoing Performance Monitoring Significant Developments Data Incidents (Cloud Data Processing Addendum)

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
10	21.	To this end, the company must ensure that its agreement with the service provider grants it the necessary rights of instruction and control.	Control You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the Services. Instructions You can provide Google instructions about your data and Google will comply with those instructions. Regulated entities have the right to issue instructions to Google. To do this, regulated entities can use the following functionality of the Services: • Cloud Console: A web-based graphical user interface that customers can use to manage their GCP resources. • gcloud Command Tool: A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer's operating system. • Google APIs: Application programming interfaces which provide access to GCP.	N/A Google's Compliance with Instructions (Cloud Data Processing Addendum) Instructions
C. Outsourcing within a group or conglomerate				
11	22.	With regard to the requirements set out in Margin nos. 16–21 and 32–35, relationships within the group or conglomerate may be considered to the extent that the risks typically associated with outsourcing are demonstrably absent or certain requirements are not relevant or are met in some other way.	This is a customer consideration.	N/A
D. Responsibility				
12	23.	The company remains accountable to FINMA in the same way as it would if it performed the outsourced function itself. Proper business conduct must be assured at all times.	This is a customer consideration.	N/A
E. Security				
13	24.	Where security-relevant functions are outsourced (particularly in information technology), the company and the service provider must contractually agree security requirements. The company must monitor compliance with these requirements.	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.	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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) ● PCI DSS ● SOC 1 ● 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:	

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **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	
14	25. The company and the service provider must draw up a security framework to ensure that the outsourced function can continue to be performed in an emergency. In doing so, the company must apply the same degree of care and attention as it would if it performed the outsourced function itself.	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
F. Audit and supervision			
15	26. The company, its audit firm and FINMA must be able to verify the service provider's compliance with supervisory regulations. They must have the contractual right to inspect and audit all information relating to the outsourced function at any time without restriction.	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. 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

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
16	27.	Auditing may be delegated to the service provider's auditors if these are adequately qualified. Where this is done, the company's audit firm may use the findings of the service provider's auditors for its audit.	Refer to Row 13 for more information on the audit reports Google provides.	N/A
17	28.	The outsourcing of a function must not make supervision by FINMA more difficult, in particular if the function is outsourced to another country.	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. Refer to Row 15 for more information on the audit, access and information rights Google grants to supervisory authorities. These rights apply regardless of the service location.	Enabling Customer Compliance
18	29.	If the service provider is not supervised by FINMA, it must enter into a contractual obligation with the company to provide FINMA with all the information and documentation concerning the outsourced functions, which are necessary for FINMA's supervisory activities. If auditing is delegated to the service provider's auditors, their report must be supplied, on request, to FINMA as well as to the outsourcing company's internal auditors and audit firm.	Refer to Row 15 for more information on the information available to supervisory authorities. Refer to Row 13 for more information on the audit reports Google provides.	N/A
G. Outsourcing to another country				
19	30.	Outsourcing to another country is admissible if the company can expressly guarantee that it, its audit firm and FINMA can assert and enforce their right to inspect and audit information.	Refer to Row 15 for more information on the audit, access and information rights Google grants to regulated entities, supervisory authorities and both their auditors. These rights apply regardless of the service location.	N/A
20	31.	The possibility of restructuring or resolving the company in Switzerland must be assured. Access to the information required for this purpose must be possible in Switzerland at all times.	Regulated entities may access their data on the services at any time in Switzerland or any other location.	Customer Information, Audit and Access
H. Agreement				
21	32.	The outsourcing must be based on a written agreement or an agreement in some other format that can be evidenced in text form. In addition to naming the parties and describing the function, this agreement must also contain the following as a minimum (Margin nos. 33–34):	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	N/A
22	33.	The company must ensure that it is informed about the use or replacement of subcontractors for significant functions at an early stage and has the possibility of terminating the outsourcing in an orderly manner in accordance with Margin no. 18.1. Where subcontractors are used, they must also be bound by the obligations and guarantees on the part of the service provider that are necessary to comply with this circular.	Changing subcontractors To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors;	Google Subcontractors

FINMA Circular 2018/3

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor. <u>Subcontractor performance</u> Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you. In particular, we recognize that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	
23	34. The agreement must include measures to ensure implementation of the requirements set out in this circular, in particular in Margin nos. 21, 24, 26, 29, 30 and 31.	Refer to Rows: 10, 13, 15, 18, 19 and 20 for more information on the implementation of requirements set out in Circular 2018/3.	N/A
24	35. The company must specify the internal approval procedures for outsourcing projects as well as the responsibilities for signing outsourcing agreements.	This is a customer consideration.	N/A