MaRisk AT 9 Outsourcing

Google Cloud Mapping

This document is designed to help institutions within the scope of the the Bundesanstalt für Finanzdienstleistungsaufsicht's (BaFin) and the Deutsche Bundesbank's supervisory mandate ("**regulated entity**") to consider AT 9 (Outsourcing) of the Minimum Requirements for Risk Management ("**framework**"), in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: AT 9(6) to AT 9(11). 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.	AT 9(6). In the case of material outsourced activities and processes, the institution, in the event of an intended or expected termination of the outsourcing arrangement, shall take safeguards to ensure the continuity and quality of the outsourced activities and processes also after the termination of the outsourcing arrangement. In cases of unintended or unexpected termination of these outsourced activities and processes that might seriously impair business activity, the institution shall examine the feasibility of and adopt possible courses of action. This shall entail, as far as meaningful and possible, defining corresponding exit processes. The courses of action shall be reviewed both regularly and on an *ad hoc* basis.	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 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.	Transition Term
2.	AT 9(7). In the case of material outsourced activities and processes, the outsourcing contract, which shall be documented in writing ("*Textform*" pursuant to section 126 of the BGB), shall specifically:	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
3.	(a) specify and, where appropriate, delineate the services to be provided by the external service provider,	The Google Cloud services are described on our services summary page.	Definitions
4.	(b) agree the start date and, as applicable, the end date of the outsourcing arrangement,	Refer to your Google Cloud Financial Services Contract.	Term and Termination
5.	(c) agree the law governing the outsourcing arrangement in those cases in which the laws of Germany do not apply,	Refer to your Google Cloud Financial Services Contract.	Governing Law
6.	(d) agree the locations (ie the regions or countries) in which the service will be performed and/or where relevant data will be kept and processed, including a requirement to notify the institution if the external service provider proposes to change the location,	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. -Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page.	Data Transfers (Cloud Data Processing Addendum)

MaRisk AT 9 Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
		-Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: -The same robust security measures apply to all Google facilities, regardless of country / region. -Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
7.	(e) define the agreed service levels, including precise performance targets,	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
8.	(f) where applicable, agree that the external service provider shall submit proof of insurance cover against certain risks,	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance

MaRisk AT 9 Outsourcing
Google Cloud Mapping

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
9.	(g) agree the requirements to implement and test business contingency 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. Regulated entities can review our plan and testing results. In addition, access information about how customers can use our Services in their own business contingency planning with our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
10.	(h) set out appropriate internal and external auditors' rights of information and review,	Google grants information, audit and access rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.	Customer Information, Audit and Access
11.	(i) ensure that the competent authorities pursuant to section 25b (3) of the Banking Act retain unrestricted information and audit rights and the ability to supervise with regard to the outsourced activities and processes,	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees.	Regular Information, Audit and Access
12.	(j) include powers to give instructions, where necessary,	Regulated entities have the right to issue instructions to Google. To do this, the 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 Google Cloud resources. gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud services. A command-line interface is a user interface to a computer's operating system. Google APIs: Application programming interfaces which provide access to Google Cloud services.	Instructions
13.	(k) include rules ensuring compliance with data protection provisions and other security requirements,	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and security of information when using a cloud service consists of two key elements:	Confidentiality

MaRisk AT 9 Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
		(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. (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; Google's Security Measures (Data Processing and Security Addendum)

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
		Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
14.	(l) specify termination rights and appropriate notice periods,	Regulated entities can terminate our contract with advance notice: • for Google's material breach after a cure period; and	Term and Termination

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
		- for change of control; and - for Google's insolvency In addition, regulated entities can elect to terminate our contract for convenience with advance notice, including: - if necessary to comply with law; and - if directed by a supervisory authority.	
15.	(m) include rules covering the possibility and modalities of subcontracting which ensure that the institution continues to comply with the prudential supervisory requirements,	Refer to Row 17 on subcontracting.	N/A
16.	(n) obligate the external service provider to inform the institution of any developments that might impair the proper performance of the outsourced activities and processes.	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
17.	AT9 (8). With respect to subcontracting, where possible, either the outsourcing institution shall be given the right to reserve approval or concrete provisions shall be agreed in the outsourcing agreement specifying when individual work and process steps may be subcontracted. At the very least, it shall be contractually ensured that the agreements the external service provider has with subcontractors are consistent with the contractual arrangements of the original outsourcing agreement. In addition, the contractual requirements shall include, in the case of subcontracting, an obligation on the part of the external service provider to provide information to the outsourcing institution. It must be ensured that, in the event that the external service provider subcontracts activities or	Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would potentially be denying all our customers the benefit motivating the subcontracting.	Google Subcontractors

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
	processes to a third party, it remains responsible for reporting to the outsourcing institution.	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google 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 competent 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.	
18.	AT9 (9) The institution shall appropriately manage the risks associated with outsourcing and shall monitor the provision of the outsourced activities and processes in a due and proper manner. In the case of the outsourcing of critical or important activities and processes, this also comprises continuously monitoring the external service provider's performance using defined criteria (eg key performance indicators, key risk indicators) and contractually agreed information supplied by the external service provider; the quality of the services provided shall be assessed on a regular basis.	You can monitor the 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. ● Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud resources and changes to resources including VM instances, images, and operating systems. ● Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud.	Ongoing Performance Management
19.	AT9 (10) The institution shall clearly specify the responsibilities for documenting, managing and monitoring material outsourced activities and processes. If special functions pursuant to number 5 are completely outsourced, the management board shall	This is a customer consideration.	N/A

MaRisk AT 9 Outsourcing

Google Cloud Mapping

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract ref.
	appoint a responsible officer for each function who shall ensure that the respective tasks are being properly performed. The requirements of AT 4.4.3 and BT 2 shall be complied with accordingly.		
20.	AT9 (11) The requirements governing the outsourcing of activities and processes shall be complied with also in the event that the outsourced activities and processes are subcontracted.	Refer to Row 17 on subcontracting.	N/A