SFSA - Regulations and General Guidelines
regarding governance, risk management and control
Google Cloud Mapping

This document is designed to help undertakings including banking companies, savings banks, members' banks, credit market companies, and credit market associations ("**regulated entity**") supervised by the Swedish Financial Supervisory Authority or 'Finansinspektionen' ("**SFSA**") to consider the Regulations and General Guidelines regarding governance, risk management and control at credit institutions ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on Chapter 10 - Outsourcing Agreements, sections 5 and 6 of the framework. 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	**Chapter 10 Outsourcing agreements - Section 5**		
2	An undertaking shall exercise due skill, care and diligence when entering into, managing and terminating outsourcing agreements relating to work or functions of material significance to the operations.The undertaking shall ensure that	Google recognizes that you need to exercise due skill, care and diligence when deciding to use our services. To assist you, we've provided information for each of the areas you may need to consider in the rows that follow.	N/A
3	1. the service provider has the skills, capacity and authorisations required by law to reliably and professionally perform the outsourced operations,	Skills ● 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 Cloud Customer page Capacity ● 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 Google's corporate and financial information on Alphabet's Investor Relations page. Authorisation Google will comply with all laws and regulations applicable to it in the provision of the Services.	N/A N/A Representations and Warranties
4	2. the service provider performs the outsourced operations efficiently and the undertaking shall to this end establish methods for assessing the performance of the service provider,	Service Levels The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. 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:	Services Ongoing Performance Monitoring

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		● 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).	
5	3. the service provider appropriately monitors its performance of the outsourced functions and management of associated risks,	Monitoring by Google Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimize the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper and on our Incidents & the Google Cloud dashboard. Independent verification 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	N/A Certifications and Audit Reports

SFSA - Regulations and General Guidelines
regarding governance, risk management and control
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You can review Google's current certifications and audit reports at any time. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	
6	4. the undertaking takes suitable measures if the service provider fails to perform the outsourced operations in an efficient manner and in accordance with applicable laws and other provisions,	Remedies If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. Termination Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period or if necessary to comply with law.	Services Term and Termination
7	5. the undertaking shall have the requisite knowledge for efficiently monitoring the outsourced operations and managing the risks that could arise in connection with the outsourcing, and monitor the outsourced operations and manage such risks,	Knowledge Google provides documentation to explain how regulated entities and their employees can use our services. If a regulated entity would like more guided training, Google also provides a variety of courses and certifications. Monitoring the service For more information on how you can monitor Google's performance of the Services, refer to Row 4. Managing the risk For information about the security measures that you can choose to implement and operate when you use the Services, refer to Row 12.	Technical Support N/A N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
8	6. the service provider has an obligation to inform the undertaking of events that could materially affect the ability of the service provider to efficiently perform the outsourced operations according to applicable laws, statutes or other regulations,	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. 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)
9	7. the undertaking informs Finansinspektionen of material changes in the outsourced operations,	Changes to the outsourced operations You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities can use the following functionality to control 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. Updates to the Service Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period. Significant developments	Instructions Changes to Services

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		For information on how Google reports developments that materially impact Google's ability to perform the Services, refer to Row 8.	N/A
10	8. the continuity and quality of the services offered by the undertaking to its customers are not affected by the termination of the outsourcing agreement,	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. 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 Data Export (Cloud Data Processing Addendum)
11	9. the undertaking, its auditors and Finansinspektionen have access to information regarding the outsourced operations and access to the premises of the service provider	Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit. In addition, regulated entities may access their data on the services at any time and may provide their supervisory authorities with access.	Regulator Information, Audit and Access Customer Information, Audit and Access
12	10. the service provider protects all confidential information relating to the undertaking or its customers, and	The confidentiality and security of information when using a cloud service consists of two key elements: Google's infrastructure	Confidentiality; Data Security; Security Measures (Cloud Data Processing Addendum)

SFSA – Regulations and General Guidelines
regarding governance, risk management and control
Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. <u>Your data and applications in the cloud</u> 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) <u>Security by default</u> 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	

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases	
13	11. the undertaking and the service provider maintain a contingency plan for reestablishing operations after unforeseen events, and for periodic testing of back-up procedures, if necessary with account taken of the parts of the operations that were outsourced.	Google will implement a disaster recovery and business contingency plan for our 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. Information about how customers can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide. In particular, as part of your contingency planning, you can choose to use build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup.	Business Continuity and Disaster Recovery
14	**Chapter 10 Outsourcing agreements - Section 6**		
15	An undertaking shall ensure that its and the service provider's rights and obligations are set forth in a written outsourcing agreement.	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A