Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

This document is designed to help insurance and reinsurance undertakings s (“**regulated entity**”) to consider Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on Article 274 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	274(1) Any insurance or reinsurance undertaking which outsources or proposes to outsource functions or insurance or reinsurance activities to a service provider shall establish a written outsourcing policy which takes into account the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented in cases of outsourcing. The undertaking shall ensure that the terms and conditions of the outsourcing agreement are consistent with the undertaking's obligations as provided for in Article 49 of Directive 2009/138/EC.	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A
2	274(2) Where the insurance or reinsurance undertaking and the service provider are members of the same group, the undertaking shall, when outsourcing critical or important operational functions or activities take into account the extent to which the undertaking controls the service provider or has the ability to influence its actions.	This is a customer consideration.	N/A
3	274(3) When choosing the service provider referred to in paragraph 1 for any critical or important operational functions or activities, the administrative, management or supervisory body shall ensure that:	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided information for each of the areas you need to consider in the rows that follow.	N/A
4	274(3) a. a detailed examination is performed to ensure that the potential service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily, taking into account the undertaking's objectives and needs;	Ability • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. Capacity • Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. • Information about Google Cloud's leadership team is available on our Media Resources page. • You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. Authorisation Google will comply with all laws and regulations applicable to it in the provision of the Services.	N/A
5	274(3) b. the service provider has adopted all means to ensure that no explicit or potential conflict of interests jeopardize the fulfilment of the needs of the outsourcing undertaking;	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct, which addresses conflicts of interest.	N/A

Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
6	274(3) c. a written agreement is entered into between the insurance or reinsurance undertaking and the service provider which clearly defines the respective rights and obligations of the undertaking and the service provider;	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract. Refer to Rows 10 to 22 for information on the contents of the written agreement.	N/A
7	274(3) d. the general terms and conditions of the outsourcing agreement are clearly explained to the undertaking's administrative, management or supervisory body and authorised by them;	This is a customer consideration.	N/A
8	274(3) e. the outsourcing does not entail the breaching of any law in particular with regard to rules on data protection;	Google will comply with all national data protection regulations applicable to it in the provision of the Services. This is addressed in the Cloud Data Processing Addendum. For more information on how Google Cloud can assist you in complying with the GDPR see our GDPR resource center.	Representations and Warranties
9	274(3) f. the service provider is subject to the same provisions on the safety and confidentiality of information relating to the insurance or reinsurance undertaking or to its policyholders or beneficiaries that are applicable to the insurance or reinsurance undertaking.	The security / confidentiality 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.	Confidentiality Data Security; Google's Security Measures (Data Processing and Security Terms)

Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(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 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	
10	274(4) The written agreement referred to in paragraph 3 (c) to be concluded between the insurance or reinsurance undertaking and the service provider shall in particular clearly state all of the following requirements:		
11	274(4) a. the duties and responsibilities of both parties involved;	The duties and responsibilities of both parties are set out in the Google Cloud Financial Services Contract.	N/A

Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
12	274(4) b. the service provider's commitment to comply with all applicable laws, regulatory requirements and guidelines as well as policies approved by the insurance or reinsurance undertaking and to cooperate with the undertaking's supervisory authority with regard to the outsourced function or activity;	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Representations and Warranties Enabling Customer Compliance
13	274(4) c. the service provider's obligation to disclose any development which may have a material impact on its ability to carry out the outsourced functions and activities effectively and in compliance with applicable laws and regulatory requirements;	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. 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 at 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 (Data Processing and Security Terms)
14	274(4) d. a notice period for the termination of the contract by the service provider which is long enough to enable the insurance or reinsurance undertaking to find an alternative solution;	Notice periods apply for termination by both you and Google. Refer to your Google Cloud Financial Services Contract	Term and Termination
15	274(4) e. that the insurance or reinsurance undertaking is able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of services to policyholders;	Regulated entities 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. In addition, regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. 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.	Term and Termination Transition Term
16	274(4) f. that the insurance or reinsurance undertaking reserves the right to be informed about the outsourced functions and activities and their performance by the services provider as well as a right to issue general guidelines and individual instructions at the address of the service provider, as to what has to be taken into account when performing the outsourced functions or activities;	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 Service Health Dashboard provides status information on the Services.	Ongoing Performance Monitoring

Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP, including availability and uptime of the services. • 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). Refer to Row 20 for more information on how you can instruct Google.	
17	274(4) g. that the service provider shall protect any confidential information relating to the insurance or reinsurance undertaking and its policyholders, beneficiaries, employees, contracting parties and all other persons;	Refer to Row 9 for more information on Google's security measures.	N/A
18	274(4) h. that the insurance or reinsurance undertaking, its external auditor and the supervisory authority have effective access to all information relating to the outsourced functions and activities including carrying out on-site inspections of the business premises of the service provider;	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. This includes access to Google's premises used to provide the Services to conduct an on-site audit. You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access.	Regulator Information, Audit and Access Customer Information, Audit and Access
19	274(4) i. that, where appropriate and necessary for the purposes of supervision, the supervisory authority may address questions directly to the service provider to which the service provider shall reply;	Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Enabling Customer Compliance
20	274(4) j. that the insurance or reinsurance undertaking may obtain information about the outsourced activities and may issue instructions concerning the outsourced activities and functions;	Refer to Rows 13 and 16 for the information Google makes available about the services. 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.	Instructions Regulator Information, Audit and Access

Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
21	274(4) k. the terms and conditions, where applicable, under which the service provider may sub-outsource any of the outsourced functions and activities;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. 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 Subcontractors
22	274(4) l. that the service provider's duties and responsibilities deriving from its agreement with the insurance or reinsurance undertaking shall remain unaffected by any sub-outsourcing taking place according to point (k).	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you. Google will remain accountable to you for the performance of all subcontracted obligations.	Google Subcontractors
23	274(5) The insurance or reinsurance undertaking that is outsourcing critical or important operational functions or activities shall fulfil all of the following requirements:		
24	274(5) a. ensure that relevant aspects of the service provider's risk management and internal control systems are adequate to ensure compliance with Article 49(2)(a) and (b) of Directive 2009/138/EC;	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. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
25	274(5) b. adequately take account of the outsourced activities in its risk management and internal control systems to ensure compliance with Article 49(2)(a) and (b) of Directive 2009/138/EC;	This is a customer consideration	N/A

Delegated Regulation (EU) 2015/35 - Solvency II

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
26	274(5) c. verify that the service provider has the necessary financial resources to perform the additional tasks in a proper and reliable way, and that all staff of the service provider who will be involved in providing the outsourced functions or activities are sufficiently qualified and reliable;	Financial resources You can review Google's corporate and financial information on Alphabet's Investor Relations page. Personnel Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees. All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Refer to our security whitepaper for more information.	Personnel Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
27	274(5) d. ensure that the service provider has adequate contingency plans in place to deal with emergency situations or business disruptions and periodically tests backup facilities where necessary, taking into account the outsourced functions and activities.	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