Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

This document is designed to help institutions supervised by the Central Bank of Brazil (“**regulated entity**”) to consider Resolution CMN 4,893 of February 26, 2021 (“**framework**”) in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Chapter III - On the contracting of services of data processing, data storage and cloud computing. 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.	Art. 11. The institutions mentioned in art. 1 must ensure that their policies, strategies and structures for risk management established in regulation in force, specifically regarding to the criteria for decision on the outsourcing of services, include the contracting of relevant data processing, data storage and cloud computing services, in the country or abroad.	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.	Art. 12. The institutions mentioned in art. 1, previously to the contracting relevant services of data processing, data storage and cloud computing, must adopt procedures that comprise:		
3.	I – the adoption of corporate governance and management practices proportional to the relevance of service to be contracted and to the risk they incur; and	The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization’s control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment. In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Board of Directors Handbook for Cloud Risk Governance and Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud.	N/A
4.	II – the verification of the capacity of the third-party provider to ensure:		
5.	a) compliance with the laws and regulations in force;	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
6.	b) the institution’s access to data and information to be processed or stored by the third party provider;	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
7.	c) confidentiality, integrity, availability and recovery of data and information processed or stored by the third-party provider;	Refer to Row 21 for more information on confidentiality, integrity, availability of data. Recovery of data and information. 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.	N/A

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. In addition, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications	
8.	d) its adherence to certifications required by the institution in order to perform the services to be contracted;	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
9.	e) the institution's access to reports provided by the specialized independent auditor hired by the third-party provider, related to the procedures and the controls used in the services to be contracted;	See Row 8 above.	N/A
10.	f) provision of adequate information and management resources to monitor the services to be contracted;	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.	Ongoing Performance Monitoring

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud 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 Google Cloud. • **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).	
11.	g) the identification and segregation of data pertaining to the institution's clients through physical or logical controls; and	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
12.	h) the quality of access controls aimed at protecting the data and information of the institution's clients;	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. • **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. • **Cloud Audit Logs** help your security teams maintain audit trails in Google Cloud 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 Google Cloud 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	N/A

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	
13.	Paragraph 1. In the assessment of the relevance of the service to be contracted, mentioned in item I of the heading, the contracting institution must consider the criticality of the service and the sensitivity of the data and information to be processed, stored and managed by the third-party provider, taking into account the classification carried out in accordance to art. 3, item V, sub-item “c”.	This is a customer consideration.	N/A
14.	Paragraph 2. The procedures mentioned in the heading must be documented, including the information related to the verification mentioned in item II.	Refer to Rows 2 to 9.	N/A
15.	Paragraph 3. In the case of applications run through the internet, referred to in item III of art. 13, the institution must ensure that the potential third-party provider adopts controls that mitigate the effects of possible vulnerabilities in releasing new versions of the application.	In addition to central source control and two-party review features, Google provides libraries that prevent our developers from introducing certain classes of security bugs. For example, we have libraries and frameworks that eliminate XSS vulnerabilities in web apps. We also have automated tools for automatically detecting security bugs including fuzzers, static analysis tools, and web security scanners. As a final check, we use manual security reviews that range from quick triages for less risky features to in-depth design and implementation reviews for the most risky features. These reviews are conducted by a team that includes experts across web security, cryptography, and operating system security. The reviews can also result in new security library features and new fuzzers that can then be applied to other future products. Refer to our infrastructure security design overview page for more information.	N/A
16.	Paragraph 4. The institution must have the necessary resources and competencies for the adequate management of the services to be contracted, including the analysis of information and use of resources provided under the terms of sub-item “f”, item II.	Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	N/A
17.	Art. 13. For the purposes of this Resolution, cloud computing services comprises the availability to a contracting institution, on demand and in a virtual form, of at least one of the following services:	Google Cloud is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy Google Cloud as part of a hybrid or multi-cloud deployment.	N/A
18.	I - data processing, data storage, network infrastructures and other computational resources that enable the contracting institution to deploy or run softwares, which may include operating systems and applications developed or acquired by the institution;	See Row 17 above.	N/A
19.	II - deployment or execution of applications developed or acquired by the contracting institution using a third-party provider's computing resources; or	See Row 17 above.	N/A

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
20.	III - execution, through the internet, of applications deployed or developed by a third-party provider using its own computational resources.	See Row 17 above.	N/A
21.	Art. 14. The institution contracting the services mentioned in art. 12 is responsible for the reliability, integrity, availability, security and confidentiality of the services contracted, as well as for compliance with the legislation and regulation in force.	Security and confidentiality 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. (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:	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

Central Bank of Brazil - Resolution CMN 4,893

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 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 Reliability and availability Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Service Level Agreements page. Compliance with legislation and regulation Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Services Representations and Warranties

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
22.	Art. 15. The contracting of relevant services of data processing, data storage and cloud computing must be communicated to the Central Bank of Brazil by the institutions mentioned in art. 1º.	This is a customer consideration.	N/A
23.	Paragraph 1. The communication mentioned in the heading must comprise the following information:		
24.	I – the name of the contracted third-party provider;	Refer to your Google Cloud Financial Services contract.	Order Form; Recitals
25.	II – the relevant contracted services; and	The Google Cloud services are described on our services summary page.	Definitions
26.	III – the designation of the countries and the regions in each country where the services can be provided and the data can be stored, processed and managed, as defined in item III, art. 16, in the case of contracting abroad.	Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available here. Refer to Row 32, for more information on where data can be stored, processed and managed.	N/A
27.	Paragraph 2. The communication mentioned in the heading must be made up to ten days after the contracting of services.	This is a customer consideration.	N/A
28.	Paragraph 3. The contractual changes that imply a modification of the information referred to in paragraph 1 must be communicated to the Central Bank of Brazil up to ten days after the change are effective.	This is a customer consideration.	N/A
29.	Art. 16. The contracting of data processing, data storage and cloud computing relevant services provided abroad must fulfill the following requisites:		
30.	I - the existence of an agreement for exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where the services may be provided;	This is a customer consideration.	N/A
31.	II - the contracting institution must ensure that the provision of the services mentioned in the heading do not cause damage to its own functioning neither do they deter the action of the Central Bank of Brazil;	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 Google Cloud resources. ● gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. 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. Google recognizes that regulated entities and their supervisory authorities must be able	Instructions Enabling Customer Compliance

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. These rights apply regardless of the service location. 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.	
32.	III - the contracting institution must define, previously to the contracting, the countries and the regions in each country where the services can be provided and the data can be stored, processed and managed; and	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. • 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 Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
33.	IV - the contracting institution must anticipate alternatives for business continuity either in the case of impossibility of continuation of the contract or in the case of its termination.	We recognize that, whatever the level of technical resilience that can be achieved on Google Cloud, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: • Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise.	Data Export (Cloud Data Processing Addendum)

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. • Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on Google Cloud across other Cloud providers or on-premise. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	
34.	Paragraph 1. In the absence of an agreement under the terms of item I of the heading, the contracting institution must request an authorization from the Central Bank of Brazil for:		
35.	I – contracting services, at least sixty days prior to the contracting, considering the terms of art. 15 of this Resolution; and	This is a customer consideration.	N/A
36.	II – contractual amendments that imply an alteration of the information provided in art. 15, Paragraph 1, at least sixty days prior the execution of the amendment.	This is a customer consideration.	N/A
37.	Paragraph 2. In order to comply with clauses II and III of the heading, the contracting institutions must ensure that the laws and regulations in the countries and regions in each country where the services may be provided do not restrict or prevent either the institution or the Central Bank of Brazil from accessing the data and information.	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Regulator Information, Audit and Access
38.	Paragraph 3. The proof of compliance with the requirements referred to on items I to IV of the heading and the fulfillment of the requirement mentioned in paragraph 2 must be documented.	This is a customer consideration.	N/A
39.	Art. 17. The contract of relevant services of data processing, data storage and cloud computing must comprise:		
40.	I – an indication of the countries and the regions in each country where services may be provided and data may be stored, processed and managed;	Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. 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). Refer to Row 32, for more information on where the services may be provided.	Data Transfers (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
41.	II – the adoption of security measures for transmission and storage of the data mentioned in item I of the heading;	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Refer to Row 21, for more information on Google's security measures..	
42.	III – the segregation of data and the access controls to protect the clients' information while the contract is in force;	Access controls Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. • **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. • **Cloud Audit Logs** help your security teams maintain audit trails in Google Cloud 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 Google Cloud 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. Segregation of data To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum) Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
43.	IV – the obligation of, in the case of contract termination:		

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
44.	a) transfer of the data cited in item 1 of the heading to the new third-party provider or the contracting institution; and	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 here and on storage options here.	Transition Term Data Export (Cloud Data Processing Addendum)
45.	b) elimination of the data mentioned in item 1 of the heading by the substituted third-party provider, after the data transfer mentioned in item 'a' and the confirmation of the integrity and availability of the received data.	On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)(Cloud Data Processing Addendum)
46.	V – the access by the contracting institution's to:		
47.	a) information provided by the third-party provider, in order to verify the compliance with items I and III of the heading;	Refer to Rows 40 to 42.	N/A
48.	b) information related to certifications and reports provided by the specialized independent audit mentioned in art 12, item II, sub-items "d" and "e"; and	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	Certifications and Audit Reports

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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.	
49.	c) proper information and management resources to monitor the services to be provided, mentioned in art. 12, item II, sub-item "f";	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 Google Cloud. • **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).	Ongoing Performance Monitoring
50.	VI – the obligation of the third-party provider to notify the contracting institution in case of subcontracting services deemed relevant to the 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 Subcontractors
51.	VII – the permission of access by the Central Bank of Brazil to the contracts and terms related to the rendering of services, the documentation and information related to the services provided, data stored and information about its processing, backup of data and information, as well as access codes to the data and information;	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. Regulated entities may access their data on the services at any time. Regulated entities may provide their supervisory authority with access. Where relevant, regulated entities may disclose a copy of the contract to their	Enabling Customer Compliance

Central Bank of Brazil - Resolution CMN 4,893

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		supervisory authority.	
52.	VIII – the adoption of measures by the contracting institution as a result of determinations from the Central Bank of Brazil; and	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	Enabling Customer Compliance
53.	IX – the obligation of the third-party provider to keep the contracting institution permanently informed about possible limitations that may affect the services provided or compliance with laws and regulations in force.	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 (Cloud Data Processing Addendum)
54.	Sole Paragraph. The contracts mentioned in the heading must comprise, in case the contracting institution is submitted to a resolution regime by the Central Bank of Brazil:		
55.	I - the obligation of the third party provider to allow full access by the responsible for the resolution regime to contracts, terms, documentation and information related to the services provided, to the data stored and information about its processing, to the data and information backup, as well as to the access codes mentioned in item VII that are available to the third party provider; and	Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Enabling Customer Compliance
56.	II - the obligation to previously inform the responsible for the resolution regime about the intention of the third party provider to interrupt the rendering of services, at least thirty days before the date of the interruption, observed that:	Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution.	Support through Resolution
57.	a) the third party provider is obliged to accept an occasional request by the responsible for the resolution regime for an additional period of thirty days before the interruption of services; and	See Row 56 above.	N/A
58.	b) the previous information also applies to an interruption motivated by a default of the contracting institution.	See Row 56 above.	N/A
59.	Art. 18. The provisions of articles 11 to 17 do not apply to contracting of systems operated by clearing and settlement systems operators or trade repositories.	This is a customer consideration.	N/A