The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

This document is designed to help institutions supervised by the State Bank of Vietnam ("**regulated entity**") to consider Circular No. 09/2020/TT-NHNN ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Section 6: Articles 32 - 36 . 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	**Article 32. General principles of use of third parties' services**		
2	When using a third party's information technology services, each institution must ensure the following principles:		
3	1. Do not reduce the institution's capacity to provide continuous services for its clients.	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. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications	N/A
4	2. Do not negatively affect the institution's control of operational procedures.	You operate the services independently without action by Google personnel. 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.	Instructions
5	3. Do not change the institution's responsibility for assurance of information security.	The security of a cloud service consists of two key elements: (1) Security of Google's infrastructure	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

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. (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	

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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	
6	4. Information technology services provided by a third party must comply with the institution's regulations on assurance of information security.	Refer to Row 5 for more information on Google Cloud's security measures.	N/A
7	**Article 33. Requirements for use of third parties' services**		
8	Before using a third party's services for information systems of level 3 or higher and information systems that process clients' personal information, each institution shall:		
9	1. Carry out an assessment of information technology risks and operating risks, including the following contents:	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 the information below.	N/A
10	a) Identify risks, analyze and estimate the extent of damage and threats to information security;	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk. 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
11	b) Define the capacity to control operational procedures, provide continuous services for clients and provide information to regulatory authorities;	Control	Instructions

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You operate the services independently without action by Google personnel. 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. Continuous services The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. Information for regulators 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.	Services Regulator Information, Audit and Access Customer Information, Audit and Access
12	c) Clearly define roles and responsibilities for assurance of service quality of relevant parties;	We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers. It is important for regulated entities to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organization and the cloud service provider. Responsibility in the cloud is assigned as follows: ● Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. ● Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications.	N/A

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers.	
13	d) Work out risk minimization methods and trouble preventing and solving methods;	In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. Our Autonomic Security Operations (ASO) solution: • delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. • enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution. Information on Google's security products is available here. Here are some examples: • **Cloud Security Scanner** automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. • **Event Threat Detection** automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment. • **Cloud Security Command Center** and **Security Health Analytics** provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.	N/A
14	dd) Review and amend risk management policies (if any).	This is a customer consideration	N/A
15	2. If an institution uses cloud computing services, apart from the provisions in Clause 1 of this Article, it shall:		
16	a) Classify activities and professional operations expected to be performed on cloud computing based on assessment of impacts of the aforesaid activities and professional tasks on operations of the institution;	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 Our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides	N/A

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk. .	
17	b) Develop backup plans for components of information systems of level 3 or higher. Backup plans must be tested and assessed to determine whether they are available to replace activities and professional tasks performed on the cloud computing;	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. Google recognizes that, whatever the level of technical resilience that can be achieved on GCP, 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. ● 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 GCP 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.	Data Export (Cloud Data Processing Addendum)
18	c) Establish criteria for selection of third parties meeting the requirements in Article 34 hereof;	This is a customer consideration.	N/A
19	d) Review, amend and apply information security methods of the institution, and limit access through cloud computing to the institution's information systems.	Security Refer to Row 5 for more information on Google's security measures. Access Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.	Data Security; Additional Security Controls (Cloud Data Processing Addendum)

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • **Cloud Audit Logs** help your security teams maintain audit trails in GCP 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 GCP 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.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
20	3. In case a third party is hired to perform all administration tasks for an information system of level 3 or higher or an information system that processes clients' personal information, the institution shall carry out risk assessment according to the provisions in Clause 1 of this Article, and send assessment reports to SBV (via the Information Technology Authority).	Refer to Rows 7 - 14.	N/A
21	**Article 34. Criteria for selection of a third party providing cloud computing services**		
22	Criteria for selecting a qualified third party shall, inter alia, include the following contents:		
23	1. The third party to be selected must be an enterprise;	Refer to our Google Contracting Entity page for information about which Google entity is the provider of the services in each country / region. Each entity is permitted to provide the services in the relevant country / region.	N/A
24	2. It owns information technology infrastructure corresponding to the service requested by the institution which must:		

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
25	a) comply with regulations of the law of Vietnam;	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties
26	b) has been granted an international certificate of information security which is still valid.	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
27	**Article 35. Conclusion of service contract with a third party**		
28	A service contract signed with a third party that shall provide services for information systems of level 3 or higher and information systems that process clients' personal information shall, inter alia, include the following contents:		
29	1. The third party's information security commitments, including:	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Refer to Row 5 for more information on Google's security measures.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)
30	a) Not to replicate, alter, use or provide the institution's data for other individuals or institutions, unless the data is provided at the request of a regulatory authority as prescribed by law; in such case, the third party is required to give a prior notice to the institution before providing its data, unless giving notice will violate the law of Vietnam;	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Protection of Customer Data

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
31	b) Disseminate the institution's regulations on assurance of information security to all staff members of the third party involving in the contract execution, and implement methods for supervising their compliance with such regulations.	Refer to Row 5 for more information on Google's security measures as well tools provided by Google that you can choose to use to enhance and monitor the security of your data.	N/A
32	2. Specific provisions on maximum allowable amount of time of service interruption and troubleshooting time limit, requirements for assurance of continuous operation (on-site backup, data backup, disaster recovery), requirements regarding processing, calculating and storing capacity as well as actions taken in case of failure to ensure service quality.	Service Interruption Google recognizes that regulated entities are expected to set impact tolerances on the assumption that a disruption will occur. Google is committed to enabling regulated entities to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article. We recognize that to remain within impact tolerances regulated entities often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud. Support/trouble-shooting The support services are described on our Technical Support Services Guidelines page. This includes hours of operation, response times and languages supported.	Business Continuity and Disaster Recovery Technical Support
33	3. Cases in which lease of a sub-contractor by the third party causes no change in responsibilities of such third party for services rendered to the institution.	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

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. In addition, Google will remain accountable to you for the performance of all subcontracted obligations.	
34	4. Data generated during the provision of service that is considered the institution's asset. When the provision of service is terminated:	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination.	Intellectual Property
35	a) The third party shall return or support the transmission of the entire data used and generated during its provision of service to the institution;	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)
36	b) The third party shall make a commitment to delete all data of the institution within a specified period of time.	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 Platform whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)
37	5. Notification of any violations against regulations on information security applied to the provided service committed by staff members of the third party.	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)

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
38	6. Apart from the provisions in Clauses 1, 2, 3, 4, 5 of this Article, a contract for use of cloud computing service shall also include the following contents :		
39	a) The third party must provide reports on audit of compliance with information technology regulations which is annually conducted by an independent audit organization during the validity of the contract;	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
40	b) The third party must provide instruments for control of cloud service quality and procedures for monitoring and control of cloud service quality;	Control You operate the services independently without action by Google personnel. 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. 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:	Instructions Ongoing Performance Monitoring

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	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, 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)	
41	c) The third party must clearly designate locations (cities or countries) for establishment of the data center outside of the territory of Vietnam which provides services for the institution;	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 GCP 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)
42	d) Responsibilities for data protection and prevention of unauthorized access to data through service distribution channels from the third party to institution must be defined;	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security Refer to Row 19 for information about the security resources, features, functionality and controls Google makes available that customers may use to secure and control access to customer data.	Data Security; Additional Security Controls (Cloud Data Processing Addendum)

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
43	dd) The third party must assist and cooperate in investigation carried out at the request of regulatory authorities of Vietnam as per law regulations;	Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Enabling Customer Compliance
44	e) Data of the institution must be separated from other clients' data used on the same technical basis provided by the third party.	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)
45	**Article 36. Institution's responsibilities for use of services provided by a third party**		
46	When using services provided by a third party, each institution shall:		
47	1. Provide, notify and request the third party to comply with the institution's regulations on information security.	Refer to Row 5 for more information on Google's security measures as well as the tools provided by Google that you can choose to use to enhance and monitor the security of your data.	N/A
48	2. Adopt procedures and arrange staff members to supervise and control services provided by the third party in order to ensure the service quality as agreed upon in the signed contract. With regard to cloud computing services, service quality must be supervised and controlled.	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. Refer to Row 40 for information about control and monitoring.	N/A
49	3. Impose the institution's regulations on information security on devices and services provided by the third party which are operated on the infrastructure managed and use by that institution.	GCP is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy GCP as part of a hybrid or multi-cloud deployment. Given the nature of the services, regulated entities do not manage the infrastructure used to provide the Services. Refer to Row 5 for more information on Google's security measures as well as the tools provided by Google that you can choose to use to enhance and monitor the security of your data.	N/A
50	4. Manage any change made to services provided by the third party, including change of supplier, change of solution, upgradation of new version, or change of the contents prescribed in Article 41 hereof; Fully evaluate impacts of such change and ensure such services are in safe working conditions.	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 control changes to your use of the services. 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. We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services.	Changes to Services

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Refer to Row 33 for information about changes to subcontractors.	
51	5. Apply measures to strictly oversee and restrict access rights of the third party when they access the institution's information systems.	Refer to Row 19 for information about the security resources, features, functionality and controls Google makes available that customers may use to secure and control access to customer data.	N/A
52	6. Supervise the third party's personnel during the process of contract execution. Whenever any violation against regulations on information security committed by a staff member of the third party is discovered, the institution must notify and collaborate with the third party in application of measures to deal with such violation in a timely manner.	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 (Cloud Data Processing Addendum)
53	7. Withdraw the right of access to the information systems granted to the third party, change keys or passwords handed over by the third party immediately after work duties are completed or the contract is terminated.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Google personnel do not require access to your passwords/credentials for the services. Therefore, regulated entities do not need to revoke access privileges on termination. Google shares best practices to help you manage your Google accounts. In addition, Google provides tools to help you secure your credentials. For example: Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud. 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 Platform whitepaper.	Deletion on Termination (Cloud Data Processing Addendum)
54	8. With regard to information systems of level 3 or higher or information systems that process clients' personal information or use cloud computing services, assessment of compliance with regulations on information security by the third party under provisions of the signed contract must be carried out. Such assessment of compliance shall be	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.	Customer Information, Audit and Access

The State Bank of Vietnam - Circular No. 9/2020/TT-NHNN

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	carried out on an annual or ad hoc basis whenever necessary. Results of information technology audit conducted by the independent audit organization may be used in such assessment.	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