Bank of Thailand - FPG 19/2599

Google Cloud Mapping

This document is designed to help financial institutions supervised by the Bank of Thailand (“**regulated entity**”) to consider the FPG 19/2599 (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on Section 5.5 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.	**5.5 Supervisory requirements on IT outsourcing**		
2.	Financial institutions must comply with laws, regulations or international standards related to the outsourced IT activities as well as the supervisory requirements on IT outsourcing as follows:	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.	Enabling Customer Compliance
3.	**5.5.1 General control requirements**		
4.	Financial institutions engaging in IT outsourcing for both types as prescribed in Clause 5.3 must put importance on the formulation of outsourcing policy, outsourcing risk management, service provider management, security of IT system and information, integrity of IT system and information, availability of IT system, and consumer protection, appropriately to the size and volume of transactions, complexity of the outsourced IT activities and associated risks as follows:	Refer to Rows 5 to 51.	N/A
5.	(1) Policy on IT outsourcing		
6.	When engaging in IT outsourcing including the use of cloud computing, financial institutions must set out strategies and policy on IT outsourcing as follows:		
7.	(1.1) Financial institutions must set out clear strategies for determination to engage in IT outsourcing, such as on grounds of business necessity as well as cost and benefit. Financial institutions must ensure that their IT outsourcing does not violate laws and regulations as prescribed by Thai supervisory authorities and those as prescribed by supervisory authorities of the country where the service providers are located, and does not give rise to any loopholes for serious frauds or cyber attacks, both internally and externally, which could severely affect business operations of the financial institutions. Moreover, such IT outsourcing should not severely affect the stability of Thai financial system.	Strategy 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. Compliance with laws Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. Security Refer to Rows 32 - 39 for more information on security. Stability 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	Representations and Warranties

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it.	
8.	(1.2)	Financial institutions must set out a clear and written policy on IT outsourcing, which must be in line with the outsourcing policy and corresponding to business strategies and competitiveness of the financial institutions. The policy must be approved by the board of directors and cover the classification of IT outsourcing, management of outsourcing risks, management of service providers, security of IT system and information, integrity of IT system and information, availability of the outsourced IT activities, customer protection, additional guidelines for critical IT outsourcing, reporting and examination etc.	This is a customer consideration.	N/A
9.	(1.3)	Financial institutions must review the IT outsourcing policy at least once a year to ensure that it is still corresponding to business strategies of the financial institutions that may have changed.	This is a customer consideration.	N/A
10.	(2)	**Risk management**		
11.		When engaging in IT outsourcing including the use of cloud computing, financial institutions must set out a framework for management of IT outsourcing risks as follows:		
12.	(2.1)	Financial institutions must set out a clear and written policy on management of IT outsourcing risks. The policy must be in line with the overall risk management framework of the financial institutions and commensurate with the size and volume of transaction, and complexity of the outsourced IT activities, as well as associated risks. The policy on management of IT outsourcing risks must be approved by the board of directors or committee with delegated authority. Furthermore, financial institutions must set out clear and written guidelines, practices, and assign responsible staff for management of IT outsourcing risks. The implementation of those guidelines and practices must be assessed regularly and the results must be reported to the board or senior management with delegated authority in a timely manner.	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
13.	(2.2)	Financial institutions must have sufficient knowledge and understanding of the outsourced IT activities as they must assess the severity of possible risks of IT outsourcing, and must have in place a system to assess, control, and manage key related IT outsourcing risks (such as strategic risk, operational risk, legal risk, and IT risk). The system should be commensurate with the size and volume of transaction, and complexity of the outsourced IT activities, as well as associated risks.	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
14.		On this, the assessment of risks of IT outsourcing, including the use of cloud computing, should cover risks associated with the control and protection of personal data (data privacy) and degree of reliance on service providers that	Data privacy Refer to Row 32 to 38 for information about the steps Google takes to protect the security of regulated entities' and their customers' information.	

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	may limit any further change or cancelation (vendor lock-in), and impact on critical systems of the financial institutions. Furthermore, for financial institutions that outsource IT activities to overseas service providers, especially activities related to data storage/processing or any arrangements with respect to data, they must also assess risks of outsourcing those activities to the overseas service providers, such as risk of being unable to access the data due to a disruption or blocking of cross-border communication network or system (information access risk) and legal risk associated with compliance with overseas regulations (cross-border compliance).	Vendor lock-in Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. 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 how Google's approach to open source can help you address vendor lock-in and concentration risk. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. Data access 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. Refer to Row 57 for information on the location of the services.	Data Export (Cloud Data Processing Addendum) Regulator Information, Audit and Access
15.	(2.3) Financial institutions must set out a framework for monitoring the effectiveness of service providers on a regular basis, a framework for monitoring any alteration made by service providers, as well as a framework for monitoring day-to-day incidents occurred with service providers. On this, financial institutions must take part in the resolution of an incident, if they consider that it may significantly affect their business operations. In addition, financial institutions must review and assess the effectiveness of service providers on a regular basis, and the results of the assessment must be reported to the committee or senior management with delegated authority in a timely manner.	Performance monitoring The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. 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.	Services Ongoing Performance Monitoring

Bank of Thailand - FPG 19/2599

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 GCP. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Alterations 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. 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. Incident reporting 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.	Changes to Services Significant Developments

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	Data Incidents (Cloud Data Processing Addendum)
16.	(2.4) Financial institutions must set out the business continuity plan, which covers IT outsourcing. The plan should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks, and the assessment of impact of outsourcing on business operations. In addition, there must be the IT disaster recovery plan to accommodate problems or incidents from IT outsourcing and to mitigate severity of the impact. Financial institutions must ensure that they have information available within the country to maintain the continuity of business operations and services provided to customers. The BCP and IT disaster recovery plan must be regularly reviewed and tested to ensure their effectiveness.	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
17.	There must also be a process for resolving problems or incidents from IT outsourcing, and those problems or incident as well as the resolutions of those problems or incidents must be reported to the committee or senior management with delegated authority in a timely manner.	Refer to Row 15 for the monitoring tools and reporting that Google provides.	N/A
18.	**(3) Service provider management**		
19.	When engaging in IT outsourcing including the use of cloud computing, financial institutions must have a framework for service provider management as follows:		
20.	(3.1) Financial institutions must set out a clear process and guidelines for selection of service providers, and must evaluate the readiness and appropriateness of the service providers to ensure that they can maintain the continuity of services and serve the needs of the financial institutions. The factors that should be considered for the evaluation are, such as IT knowledge, experience, internal management system, potential and capability to provide services both under usual and unusual circumstances, especially in case where the service providers have a number of clients (concentration risk).	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. Knowledge and experience • 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. • 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 is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are	N/A

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. Internal controls Refer to Row 21 on Google's internal controls. Continuity Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes.	
21.	On this, when selecting cloud computing service providers, financial institutions should consider readiness and service standards of the service providers as they should be certified according to relevant international standards, such as international standards on system and information security	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
22.	(3.2) Financial institutions must prepare a written IT outsourcing contract, or a written service level agreement in case where service providers are companies in the same group. The contract/agreement should clearly detail roles, duties, responsibilities of service providers, and service conditions, as well as responsibilities for any damage in case where the service providers fail to	The roles, duties and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	N/A

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	comply with the service conditions as specified in the contract/agreement. The contents of the contract/agreement should cover the following key information:		
23.	– Scope of the outsourced IT activity and conditions of the service provided by the service provider	The GCP services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions
24.	– Minimum operating standards as required from the service provider (such as standard on information security and confidentiality, prohibition on use of information apart from that as specified in the contract/agreement, integrity of IT system and information, and availability of the outsourced activity)	Security and confidentiality This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Data use 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. Availability and integrity The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Data Security; Google's Security Measures (Cloud Data Processing Addendum) Protection of Customer Data Services
25.	– Internal control system of the service provider	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	Certifications and Audit Reports
26.	– Contingency plan of the service provider, which should be consistent with the contingency plan of the financial institution	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

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
27.	– Reporting of operations performed by the service provider, which should cover problems or incidents from providing the service	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)
28.	– Responsibilities and obligation between the financial institution and service provider in case of problems, conditions or guidelines on change or cancellation of the contract/agreement, such as when the service provided by the service provider has ended or is canceled, the information of customers of the financial institution and that of the financial institution must be destroyed	Termination Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period. In addition, 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. Transition 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. Deletion 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.	Term and Termination Transition Term Deletion on Termination (Cloud Data Processing Addendum)
29.	– Rights of the financial institution, internal auditors, external auditors and the Bank of Thailand to request relevant information and to examine the operation and internal control of the service provider, for both domestic and overseas 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.	Regulator Information, Audit and Access Customer Information, Audit and Access
30.	Furthermore, financial institutions must keep the contract/agreements at their offices available for the examination by the Bank of Thailand or for submission as requested by the Bank of Thailand.	Where relevant, regulated entities may disclose a copy of the contract to their supervisory authority.	Enabling Customer Compliance; Information
31.	In cases where overseas service providers and supervisory authorities in any particular country impose constraints on the examination of such service providers, or where the laws or supervisory regulations differ from those as	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

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	prescribed by the Bank of Thailand, which makes financial institutions to further comply with the laws, regulations and guidelines as prescribed by those supervisory authorities, the Bank of Thailand reserves rights to impose any other supervisory regulations and/or conditions as deemed appropriate.	In addition, Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. These rights apply regardless of the service location.	Customer Information, Audit and Access
32.	**(4) System and information security**		
33.	When engaging in IT outsourcing including the use of cloud computing, financial institutions must have system and information security measures as follows:		
34.	(4.1) Financial institutions must ensure that service providers have a framework or standards on system and information security, for both information of customers and that of the financial institutions, which should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. On this, financial institutions may require service providers to apply the best practices on IT security that are in accordance with international standards and generally accepted, as deemed appropriate.	System and information security. 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	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 International standards 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	

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
35.	On this, for financial institutions engaging in cloud computing, they must ensure that cloud computing service providers have a framework on security of critical or sensitive information of customers and that of the financial institutions in accordance with international standards, such as data encryption and key management	Encryption is central to Google's comprehensive security strategy. We provide certain encryption by default, with no additional action required from 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. We also offer a continuum of encryption key management options to meet your needs. Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage, and rotation. You can choose to use these encryption and key management tools provided by Google: • Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. • Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. • Customer-managed encryption keys for Cloud SQL and GKE persistent disks. • Cloud External Key Manager lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Key Access Justification works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set.	
36.	(4.2) Financial institutions must have in place a process, procedures or systems for monitoring, evaluating and examining service providers to ensure that the service providers are able to comply with the framework or standards on security of system and information as agreed upon with the financial institutions.	You can 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. 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 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
37.	(4.3) Financial institutions must have in place a process, procedures or systems for retrieving all information of customers and that of the financial institutions from service providers. In addition, financial institutions must ensure that service providers have a process, procedures and systems for destroying information	Retrieval 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:	Data Export (Cloud Data Processing Addendum)

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		of customers and that of the financial institutions when the outsourcing agreements have ended or are canceled.	• **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. Deletion 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)
38.	(4.4)	Financial institutions must ensure that service providers have a framework or standards for taking care of and safeguarding important information of customers and that of the financial institutions, which should be in accordance with the relevant laws, supervisory regulations and international standards.	Refer to Rows 33 - 36 for more information on the steps Google takes to secure your information as well as the tools Google makes available to you to secure your data and applications.	N/A
39.	**(5)**	**System and information integrity**		
40.		When engaging in IT outsourcing including the use of cloud computing, financial institutions must have system and information integrity measures as follows:		
41.	(5.1)	Financial institutions must arrange to ensure that service providers have a framework or standards on system and information integrity, covering a process of system development or replacement, input validation, processing control and output control, as well as must arrange to ensure that the outsourced IT activities are effective, accurate and reliable. This should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. On this, financial institutions may require service providers to apply the best practices on IT security that are in accordance with international standards and generally accepted, as deemed appropriate.	System and information integrity Google's global scale infrastructure is designed to provide security through the entire information processing lifecycle. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. Our infrastructure security page describes the security of this infrastructure in progressive layers starting from the physical security of our data centers, continuing on to how the hardware and software that underlie the infrastructure are secured, and finally, describing the technical constraints and processes in place to support operational security. International standards 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.	N/A

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
42.	(5.2)	Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with the framework or standards on system and information integrity as agreed upon with the financial institutions.	Refer to Row 36 for information about how you can monitor the integrity of our services.	N/A
43.	**(6)**	**Availability of outsourced IT activities**		
44.		When engaging in IT outsourcing including the use of cloud computing, financial institutions must manage to ensure the availability of the outsourced IT activities as follows:		
45.	(6.1)	Financial institutions must ensure that service providers have a framework and standards to ensure the availability of the outsourced IT activities under usual and unusual circumstances. This should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. On this, financial institutions may require service providers to apply the best practices on IT security that are in accordance with international standards and generally accepted, as deemed appropriate.	Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes. In addition, Google proactively performs resilience testing, dependency identification, and mapping to find potential single points of failure, and then works proactively to correct any issues to minimize the impact of disruptions on customers. Services at Google are continuously monitored for their availability and graded against their SLO metrics. More information is available in our Infrastructure Design for Availability and Resilience whitepaper	Business Continuity and Disaster Recovery
46.	(6.2)	Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with a framework or standards on availability of the outsourced IT activities as agreed upon with the financial institutions.	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 GCP, including availability and uptime of the services.	Ongoing Performance Monitoring
47.	**(7)**	**Consumer protection**		

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
48.		When engaging in IT outsourcing including the use of cloud computing, financial institutions must make the arrangements with respect to customer protection as follows:		
49.	(7.1)	Financial institutions must ensure that service providers will not disclose information of customers and that of the financial institutions to other parties without consent of the financial institutions.	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
50.	(7.2)	Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with a framework or standards on customer protection as agreed upon with the financial institutions.	Given the nature of the services, Google does not have direct interaction with the regulated entity's customers. 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.	N/A
51.	(7.3)	Financial institution must have in place sufficient and appropriate systems for taking care of and managing customer complaints. The resolutions of those complaints must be reported to the committee or senior management with delegated authority in a timely manner. On this, in case where customers encounter losses from the outsourcing of financial institutions, the financial institutions must make compensation to those customers as deemed appropriate.	This is a customer consideration.	N/A
52.	**5.5.2**	**Specific control requirements**		
53.		Where financial institutions engaging in critical IT outsourcing, such as outsourcing of core banking function, data center and network system, **including the use of cloud computing for critical activities**, the financial institutions must comply with the general control requirements as prescribed in Clause 5.5.1 and must also have additional controls, which are in line with the best practices on IT security, in accordance with international standards, and generally accepted. This should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks, under the appropriate supervision of the board of directors, as follows:	Refer to Rows 54 to 60.	N/A
54.	**(1)**	**Specific risk controls**		
55.	(1.1)	Financial institutions must ensure that service providers have a process, procedures, controls on risk management, which should, at least, cover the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, and should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. In addition, service providers should be certified in accordance with international standards, such	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)	Certifications and Audit Reports

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
		as the standards of the International Organization for Standardization (ISO) and the Telecommunication Industry Association (TIA).	• 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.	
56.	(1.2)	Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with the framework or relevant international standards as agreed upon with the financial institutions. Moreover, financial institutions must conduct a test to ensure that their engaging in critical IT outsourcing will not incur any risks, according to the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, or lead to loopholes for frauds and/or cyber attacks, both internally and externally, which may severely affect the business operations or key financial services of the financial institutions on a wide scale, such as conducting a penetration test for internet banking system services.	Google is audited at least once a year for each audited framework. 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. In addition, You can perform penetration testing of the Services at any time without Google's prior approval. Google also engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Certifications and Audit Reports Customer Penetration Testing
57.	(1.3)	Financial institutions engaging in critical IT outsourcing, including the use of cloud computing for critical activities, must require service providers to provide details of locations where data of the financial institutions is stored, processed or arranged (data location) in order that the financial institutions can appropriately manage outsourcing risks associated with data. In addition, financial institutions must have in place a contingency plan in case where cloud computing service is not available, and must conduct a test for that plan before using that service to ensure that the financial institutions can maintain the continuity of financial services according to the specified policy and business continuity plan.	Location To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual 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.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

Bank of Thailand - FPG 19/2599

Google Cloud Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
			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. Contingency plans We recognize 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 commit to open source and common standards.	Data Location (Service Specific Terms)
58.	**(2)**	**Board oversight**		
59.	(2.1)	Financial institutions must present details of critical IT outsourcing as well as results of risk assessment to the board of directors or committee with delegated authority for approval before entering into critical IT outsourcing arrangements, or when there are significant revisions to those arrangements according to the internal guidelines, or when those arrangements are renewed.	This is a customer consideration.	N/A
60.	(2.2)	Financial institutions must report the following to the board of directors or committee with delegated authority in a timely manner: the results of evaluation, monitoring and examination of service providers, according to the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, as well as problems or incidents or complaints from outsourcing.	This is a customer consideration.	N/A