Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

This document is designed to help financial institutions supervised by the Bank of Thailand ("**regulated entity**") to consider the Announcement of Bank of Thailand No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions ("**framework**") in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Third Party Risk Management Implementation Guidelines, Part 2. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Workspace services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	**1. Risk Assessment from Service Usage, Connection, or Accessing Information from the Third Party**		
2.	7.1 FI shall assess the risks and effects both before and after the Service Usage, Connection, or Accessing Information from the third party, and upon any significant changes, including regular assessment cycle of Service Usage, Connection, or Accessing Information from the third party. In this regard, the assessment result shall be made in writing by considering the following risks:	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
3.	(1) Strategic risk	Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
4.	(2) Risk concerning the governance and the management on the third party, which is not fully covered and is not precisely done.	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
5.	(3) Reputation risk, such as errors on the system and services that are jointly operated with the third party that affects the services, including the reputation and reliability of the financial institution.	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. You can review information about Google's historic performance of the services on our Google Workspace Status Dashboard.	N/A
6.	(4) Risk relating to information technology and cyber threats, such system errors or system suspension due to the third party, the third party's system having the security	Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	vulnerability which result in data loss or leakage, the third party's exercising excessive rights than permitted, and insufficient system resources.	automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated.	
7.	(5) Legal and regulatory compliance risk in the country and overseas, such as non-compliance with the Electronic Transactions Act, Computer Crime Act, Personal Data Protection Act, Cybersecurity Act, Copyright Act, and the EU General Data Protection Regulations (GDPR).	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. Google will comply with all national data protection regulations applicable to it in the provision of the Services.	Representations and Warranties
8.	(6) In-country and cross border risk in which the third party is located or is operating the business, including the aspects of politics, economics, and society, such as an inability to access the information due to an error or blockage from the cross-border communication networks.	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 is available here. • Information about the location of Google's subprocessors' facilities is available here. 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 Trusting your data with G Suite whitepaper.	Data Location (Service Specific Terms)
9.	(7)Contractual risk, such as application, clarity, and completeness of the agreements or terms.	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
10.	(8) Third party or vendor locked-in risk by dependency on one third party which could result in restrictions on changes of technology adopted by the service provider or the business partner and restrictions on operation of the system or information by the financial institution.	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 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 the transition term. More information is available on our Google Account help page.	N/A
11.	(9) Concentration risk, such as FI and its affiliates using the service from a single service provider.	See Row 10 for more information on Google's approach to concentration risk.	N/A
12.	(10) Risk on third -party subcontractors, such as an operation fault of a subcontractor.	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 (including the audit and access rights).In addition, Google will remain accountable to you for the performance of all subcontracted obligations.	Google Subcontractors
13.	7.2 FI should establish control and risk management covering the third party management life cycle covering the selection, agreements or contractual terms preparation, and ongoing monitoring, the cancellation/termination of agreements or contractual terms, including information technology security as set out under Clause No. 8-12 below.	Control and risk management You operate the services independently without action by Google personnel. You decide which services to use, what information you provide and for what purpose. Therefore you stay in control of the treatment of your data. Information about Google's approach to risk management is available in Google's certifications and audit reports. Monitoring You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.	Instructions Certifications and Audit Reports Ongoing Performance Monitoring

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		For example: • The **Status Dashboard** provides status information on the Services. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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). 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. Information Security Refer to Row 21 for more information on Google's security measures.	Term and Termination
14.	**2. Third Party Selection**		
15.	8.1 FI shall have clear regulations and criteria on consideration of the third party selection in writing which contain sufficient information to support the consideration processes on Service Usage, Connection, or Accessing Information from the third party	This is a customer consideration.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	in order to select the third party which is qualified in conformity with the objectives of FI in respect of its operation.		
16.	8.2 With regard to the decision making processes on Service Usage, Connection, or Accessing Information from the third party which have high level of risk or have materiality, it shall obtain the approval from the board of directors or executives.	Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
17.	8.3 FI shall conduct due diligence on the Third Party which cover the assessment in line with risk level and materiality level relating to Service Usage, Connection, or Accessing Information from the third party which include the following matters:	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
18.	(1) Financial status, reputation, knowledge, experience, and service provision capability of the third party in the past.	Financial status • You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. • You can review Google's audited financial statements on Alphabet's Investor Relations page. Reputation • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Workspace Cloud Customer page. Knowledge, experience and capability • 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. • You can review information about Google's historic performance of the services on our Google Workspace Status Dashboard.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
19.	(2) Governance and organization culture of the third party.	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct.	N/A
20.	(3) Risk management, internal control, internal audit, and operation monitoring.	Risk management and internal control Information about Google's approach to risk management and its internal control environment is available in Google's certifications and audit reports. Operation 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: • The **Status Dashboard** provides status information on the Services. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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).	Certifications and Audit Reports Ongoing Performance Monitoring

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
21.	(4) Information technology security.	The security 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:	(Cloud Data Processing Addendum)

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace 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	
22.	(5) Business continuity management and readiness to cope with any threats or events.	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
23.	(6) Legal and regulatory compliance, such as a request on a review of the evidence or certificate from the third party in relation to legal compliance.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.	Representations and Warranties

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24.	(7) International technology compliance standard, such as a request for ISO 27001 certificate. International compliance standard should consider that the third party is certified in relation to material part of its services, such as a computer center and/or certification which would cover the whole organization.	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) • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
25.	(8) External factors that may have impact to the service of the third party, such as the political situation, economic situation, legal limitations of the country where the third party is located or operates its business.	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. Information about the location of Google's facilities and where individual Google Workspace services can be deployed is available on our Global Locations page. 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.	N/A
26.	(9) Open technology application in order to enable the system to work with or connect with other systems (Interoperability) and to reduce restrictions for the FI to transfer or change of technology of the service provider or partners, including the limitation on operating the system or transfer of information by the FI, such as information transmission format with the third party is the open standard (Open Standard or Open Source).	Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	(Cloud Data Processing Addendum)
27.	**3. Preparation of Agreement or Terms on Service Usage, Connection, or Access Information from Third Party**		

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
28.	9.1 FI shall prepare agreements or terms on Service Usage, Connection, or Access Information from the Third Party in writing and keep such agreements or terms at FI's premise for legal enforcement and the audit readiness or upon request by Bank of Thailand.	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract. Where relevant, regulated entities may disclose a copy of the contract to their supervisory authority.	Enabling Customer Compliance
29.	9.2 FI shall incorporate any material details and conditions into agreements or agreed terms with the third party in an explicit manner by taking the risk level and the materiality of Service Usage, Connection, or Access Information from the third party into consideration, which shall include the following matters:		
30.	(1) Scopes of Service Usage, Connection, or Access Information from the Third Party	The Google Workspace 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
31.	(2) Roles, duties, and responsibilities of the third party and FI.	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. 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.	N/A
32.	(3) Minimum practical standard of the third party, such as the standard of the internal control, confidentiality of the system and information (Confidentiality), integrity of	Refer to Row 21.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	system and information (Integrity) and availability of information technology (Availability), and the standard on the consumer protection.		
33.	(4) Information technology emergency plan for Service Usage, Connection, or Access Information from the Third Party that must be consistent with the information technology emergency plan of FI.	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**
34.	(5) Monitoring and reporting of the operation result of the third party (Ongoing Monitoring) covering notifications of important changes or events, and reports of unusual events caused by Service Usage, Connection, or Access Information from the Third Party.	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: • The **Status Dashboard** provides status information on the Services. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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). Notifications	Ongoing Performance Monitoring

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Status 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
35.	(6) Personal data protection of information of FI and consumers must be set out in accordance with the relevant laws and regulations.	Google will comply with all national data protection regulations applicable to it in the provision of the Services.	Representations and Warranties
36.	(7) Destruction of information upon termination or cancellation of Service Usage, Connection, or Access Information from Third Party, such as requirement on a certificate issued by the the third party upon information of FI being destroyed.	On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems.	Deletion on Termination
37.	(8) Conditions or rights of the FI to amend, terminate or cancel the agreements or the contractual terms upon any amendment or breach of the agreements or the terms, such as the change of owner, breach of security or confidentiality, and the third party being in the process of receivership, liquidation or insolvency.	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period, for change of control and for Google's insolvency.	Term and Termination
38.	(9) Guideline relating to dispute resolution and liability on damages.	Dispute resolution Refer to your Google Cloud Financial Services Contract. Liability Refer to your Google Cloud Financial Services Contract.	Governing Law Liability
39.	(10) Audit right of the financial institution, Bank of Thailand, or the external auditor appointed by FI or BOT for being able to audit the operation and the internal control of the third party in relation to Service Usage, Connection, or Access Information from the Third Party of FI.	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
40.	9.3 In case of service which is material information technology outsourcing of the third party, FI shall stipulate rights of FI on the approval of subcontracting, and the requirement that the third party shall be responsible for the subcontractor's operation.	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:	Google Subcontractors

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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 requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Google will remain accountable to you for the performance of all subcontracted obligations.	
41.	9.4 In the event that Service Usage, Connection, or Access Information from the Third Party is located overseas, the agreements or terms on Service Usage, Connection, or Access Information from the Third Party shall take into account the possible country risk and obstructions may occur in the country where the third party is located or operates its business (Country Risk).	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 is available here. • Information about the location of Google's subprocessors' facilities is available here. 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 Trusting your data with G Suite whitepaper.	Data Location (Service Specific Terms)
42.	**4. Monitoring of Performance of the Third Party**		

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
43.	10.1 FI shall appoint the person who will be responsible and continuously monitors work performance of the third party by considering the risk level and the material level of Service Usage, Connection, or Access Information from the Third Party, such as requirement of reporting on regular basis by the third party, arrangement of the meeting, and observance of operation by the third party.	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. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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
44.	10.2 FI shall stipulate that the third party must report any unusual event which may arise during the work operation in connection with Service Usage, Connection, or Access Information from the Third Party to FI in a timely manner for acknowledgement and assessment of the possible effect to FI. However, in the event that the effect to the business operations of FI is material, FI shall participate in a decision making to resolve such usual event.	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Status 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

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

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

45.	10.3 FI shall conduct the capability assessment, the performance assessment, and the risk assessment of Service Usage, Connection, or Access Information from the Third Party, including the efficiency, the information technology security, and legal compliance upon renewal of agreements and upon the life cycle as stipulated by FI. In this regard, Service Usage, Connection, or Access Information from the Third Party that is material must have assessment at least once a year, including report of the assessment to the board of directors or executives.	Even before you are on Google Cloud, you can use our Risk Assessment & Critical Asset Discovery solution to evaluate your organization's current IT risk, identify where your critical assets reside, and receive recommendations for improving your security posture and resilience.
		
		Once on Google Cloud, you can leverage these tools to assess and manage your cloud resources on an ongoing basis:
		
		• **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.
		
		• **Configuration Manager** assists with:
		  ○ Configure which users, groups, and other data to synchronize.
		  ○ Set up rules to omit data, such as users or groups, from a sync.
		  ○ Set up notifications and logging.
		
		• **Admin Audit Logs** - you can use the Admin audit log to see a record of actions performed in your Google Admin console. For example, you can see when an administrator added a user or turned on a Google Workspace service.
			N/A

46.	**5. Cancellation or Termination of Agreement or Terms**		
47.	11.1 To set the standard or guideline regarding the cancellation or termination of the agreements or the terms as a guideline for the cancellation or termination of the agreements or the terms by taking into consideration the continuity of services and the information technology security. In this regard, such standard or guidelines must cover the roles and duties of the related committees and work units, the processes and the internal control, such as information backup prior to cancellation, deletion or recovering of the important properties of FI (e.g., information, information access key, user account).	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	Term and Termination

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	Transition Term
48.	11.2 When cancelling or terminating the agreements or the terms, FI shall assess the consequence and risk that may arise due to the cancellation or the termination on the agreements or the terms, and shall proceed in accordance with the guideline regarding the cancellation or termination of the agreements or the terms, and shall set the clear exit strategy and exit plan of cancellation or termination of the agreements or the terms, such as the service suspension of the system which has effect to customers or users, or the information technology security.	Refer to Row 47.	N/A
49.	**6. Information Technology Security on Service Usage, Connection, or Accessing Information from the Third Party**		
50.	FI shall ensure the Service Usage, Connection, or Access Information from the Third Party that the information technology security is in compliance with Three Lines of Defense for the security of the system and information (Confidentiality), the reliability of the system and the information (Integrity), and the availability of the information technology or CIA which shall be in consistent with the information technology security policy (IT Security Policy) and other related international standards regarding the information technology security, such as ISO/IEC 27001, ISO/IEC 27017. It shall comply with the guideline of the Bank of Thailand Re: Guideline on Information Technology Risk Management Implementation, including the generally accepted international standard regarding the cyber security protective and recovery plan against cyber threats, which shall be in compatible with the risk level and the materiality level of Service Usage, Connection, or Access Information from the Third Party. In this regard, in case of Cloud Computing, FI shall adopt the good practice of the cloud computing service provider to be the operational practice, and ensure that the cloud computing system has the	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) • SOC 1 • SOC 2 • SOC 3	Certifications and Audit Reports

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	information technology security, and shall proceed with the following additional control practices:	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. For information on Google's security measures and certifications refer to Row 21.	
51.	**12.1 To prepare the records of Service Usage, Connection, or Access Information from the Third Party and records of the related information technology assets.**		

52.	(1) To have the responsible department to prepare and update the records of Service Usage, Connection, or Access Information from the Third Party and the records of the related information technology assets for FI being able to specify the risk level from Service Usage, Connection, or Access Information from the Third Party and able to manage the information technology assets in a timely manner, such as consideration of related risks relating to cyber threats, or planning for a termination of agreements or terms.	You can leverage these tools to assess and manage your cloud resources on an ongoing basis:
		• **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.
		• **Configuration Manager** assists with:
		  ○ Configure which users, groups, and other data to synchronize.
		  ○ Set up rules to omit data, such as users or groups, from a sync.
		  ○ Set up notifications and logging.
		• **Admin Audit Logs** - you can use the Admin audit log to see a record of actions performed in your Google Admin console. For example, you can see when an administrator added a user or turned on a Google Workspace service.
			N/A

53.	(2) Records of Service Usage, Connection, or Access Information from the Third Party and records of the related information technology assets shall cover:		
54.	• Name of the Third party	Refer to our Google Contracting Entity page for information about which Google entity is the provider of the services in each country.	N/A
55.	• Type of the Third party, such as the Third party that is in a group of FI, the Third Party that is out of a group of FI, and the regulator.	Refer to Row 54.	N/A
56.	• Name of service/work system	Google Workspace is a public cloud service. It provides Software as a Service. Customers can choose to deploy Google Workspace as part of a hybrid or multi-cloud deployment.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
57.	• Characteristics and scope of work	The Google Workspace 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
58.	• Category of Service Usage, Connection, or Access Information from the Third Party, such as IT Outsourcing Cloud Computing, Mutual service with the business partner, the service usage of public network, the service usage of the central payment system service provider.	Refer to Rows 56 and 57.	N/A
59.	• Risk level and material risk of Service Usage, Connection, or Access Information from the Third Party	This is a customer consideration.	N/A
60.	• Location of the main and backed up computer center of the third party that are processing, collecting information, or any proceedings in relation to information or system of FI.	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 is available here. • Information about the location of Google's subprocessors' facilities is available here. 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 Trusting your data with G Suite whitepaper.	Data Location (Service Specific Terms)

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
61.	• Commencement date and termination date of the agreements or the terms of Service Usage, Connection, or Access Information from the Third Party.	Refer to your Google Cloud Financial Services Contract.	Term and Termination
62.	• Certificates in accordance with the related international standard regarding information technology (if any).	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) • 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
63.	• Details of the related assets of Service Usage, Connection, or Access Information from the Third Party, such as the information that is collected or processed, and the confidentiality classification.	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.	N/A
64.	**12.2 Information Security**		
65.	(1) To encrypt information that is under the procession of the third party in a manner that is in compliance with the policy and the standard of FI and is consistent with the international standard in accordance with the information classification, and to cover both data that is located in the operating devices (Data at Endpoint), data that is being transmitted (Data in Transit), and data that is located in system and media record (Data at Rest), including the backed-up data.	Encryption is central to Google's comprehensive security strategy. We provide certain encryption by default, with no additional action required from you. We also offer a continuum of encryption key management options to meet your needs. For more information on Google Workspace encryption and key management tools provided by Google, see our Google Workspace encryption whitepaper.	N/A
66.	(2) To self-manage the data access key of FI, which shall have control over every processes, together with the management of cryptographic keys (Lifecycle of	Google Workspace uses the latest cryptographic standards to encrypt all data at rest and in transit between our facilities by default.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Cryptographic Keys), including creation, collection, usage, backing up, revocation, and renewal of cryptographic keys	In the default mode, Google manages cryptographic keys on behalf of its customers. With Google Workspace Client-side encryption, Google is giving customers direct control of encryption keys, thereby making customer data indecipherable to Google. Google Workspace Client-side encryption (CSE) allows you to secure Drive, Docs, Sheets, and Slides data with an external encryption key that Google servers cannot access. The product is built around the following principles: • No access to plain-text content: File content is encrypted in the browser before being sent to Google servers for storage. Google cannot unilaterally access content. For example, if Google needs to access a decrypted file for support reasons, it requires explicit customer authorization on a per-file basis. • Customer sovereignty of encryption keys: To use CSE, customers need to independently set up their encryption key access service by using one of the partners that have built their services to CSE specifications. • Preserve user experience: End users can interact with web-based experiences for editing documents. They can also share files externally or access them on mobile devices.	
67.	(3) To self-create the cryptographic keys. If FI cannot create the cryptographic keys by itself, FI shall ensure that the cryptographic keys of the third party may not be jointly used with other users and shall understand the details in relation to the system of the third party's cryptographic keys management which are as follows:	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
68.	• Category of cryptographic keys.	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
69.	• Details of the system, including the control process of the information encryption on each processes along with the lifecycle management of cryptographic keys.	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
70.	• Suggestion on use and control of encrypting information.	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
71.	(4) To collect the cryptographic keys in the security device, such as Hardware Security Module (HSM) and to secure the security device of such HSM device by setting the safe network zone and limiting the connection with the unrelated additional work systems.	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
72.	(5) To audit the procedures of the management of the encryption both conducted by FI and by the third party which shall cover the vulnerability and the risk of the encryption by	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	taking into consideration of the consistency with the generally accepted international standard, such as the encryption algorithm, and the length of the encryption key.		
73.	**12.3 Access Control**		
74.	(1) To set up the procedures in writing on management and control of rights to request and access the system and information of FI to be in compliance with the information technology security policy stipulated by FI and the generally accepted international standard.	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. 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.	(Cloud Data Processing Addendum)
75.	(2) To clearly set out the roles, duties, and responsibilities of the persons who have rights to use the system and users who have the privilege rights.	Refer to Row 74.	N/A
76.	(3) To manage the right granting of the third party by limiting the rights in accordance with roles and necessity on usage, to have the approval upon request to prevent a person to perform from the beginning to the end of the whole processes.	Refer to Row 74.	N/A
77.	(4) To have a system or monitoring process of the user accounts who have the privilege rights, including to monitor and to audit the status of rights and usage or access of the data system upon cycle period which is in consistent with the risk and right necessity on regular basis to ensure that the use of rights being within the scope of authorization and the necessary usage.	Our Risk and Compliance as Code (RCaC) Solution stack enables compliance and security control automation through a combination of Google Cloud Products, Blueprints, Partner Integrations, workshops and services to simplify and accelerate time to value.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Through the RCaC solution, customers can introduce automation via IaC (Infrastructure as Code) and PaC (Policy as Code) in the form of blueprints. This lays the foundation of preventative controls. The next level of maturity is detection as code which involves monitoring for (security and compliance) drifts and applying remediations when an out-of-compliance infrastructure is identified. This forms a continuous monitoring loop that helps prevent misconfigurations.	
78.	(5) To stipulate the user identification processes by the processes which is in consistent with policy standard of FI or the generally accepted international standard.	Refer to Rows 74-77 for more information on access management.	N/A
79.	(6) In case that the third party connects with the system of FI through the system remote access, FI shall have the management over the system remote access by safe means as follows:		
80.	• To strictly obtain the approval prior to the system remote access by the user account who has the privilege rights. It is permitted only for the necessity and it is limited on the duration of system access.	Refer to Row 74-77 for information on access management.	N/A
81.	• To identify the user by two-factor authentication and to have connection through virtual private network (VPN).	Refer to Row 74-77 for information on access management.	N/A
82.	• To control the access through the permitted devices and to use the virtual desktop infrastructure for reducing the risk on malware or inappropriate access to the system.	Refer to Row 74-77 for information on access management.	N/A
83.	• To be able to specify and to audit the source of devices or system which remotely connect with the system of FI.	Refer to Row 74-77 for information on access management.	N/A
84.	• To audit the remote access system by user accounts with the privilege rights with the person or by the organization who is independent and has appropriate knowledge.	Refer to Row 74-77 for information on access management.	N/A
85.	(7) To manage and cause the third party to collect the history of user authentication, access log, and activity log in accordance with the period as required by laws and to audit the records in accordance with the cycle which is compatible with the risk and the materiality regularly to ensure that the third party operates in accordance with the terms and the information technology security standard of FI.	Refer to Row 74-77 for information on access management.	N/A
86.	**12.4 Communication Security**		

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
87.	(1) To have security on the data transmission through the communication network with the third party subject to the information technology security policy, together with the generally accepted international standard.	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.	N/A
88.	(2) To oversee and cause the third party to put in place the system or process for traffic screening that are submitted through the network, detection, notification, and being able to suppress the intrusion or to respond to incursions automatically and continuously on the network system to be compatible with the risk level and the materiality level of Service Usage, Connection, or Access Information from the Third Party, such as having the network intrusion detection and prevention systems (NIDPS), Web application firewall (WAF), Protection policy on attacks in relation to the distributed denial of services (DDoS), and Data leakage prevention systems (DLPS) and having the scanning of other viruses or malwares that intrude the system.	At Google we rely on a zero trust system known as BeyondCorp, to move beyond the idea of a privileged corporate network. For more information on our zero trust approach refer to our What is Zero Trust Identity Security? blog post. 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. 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: • Alert Center provides real-time actionable alerts and security insights about activity in your Google Workspace domain. • Cloud Identity is a unified identity, access app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximize end-user efficiency and protect your organization's data.	N/A

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Security Center provides actionable security insights for Google Workspace to help protect your organisation.	
89.	(3) In case of use of the cloud computing, the service provider shall detach the environment of FI from other users who are jointly in the cloud computing environment.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	N/A
90.	**12.5 Change Management**		
91.	(1) To jointly set out procedures and guidelines on the change of management with the third party which would allow FI to be able to assess the consequence and to prepare the reservation options, such as upon change of system of the Cloud Computing service provider which affecting the services of FI.	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.	Changes to Services
92.	(2) To require the third party to inform the change of the information technology that may affect the service of FI within the agreed period in order to allow FI to determining available options to reduce the effect to the consumers.	Refer to Row 91.	N/A
93.	**12.6 System Configuration Management**		
94.	In case the third party have the duties on the change of system settings, FI shall set the system setting standard to be sufficiently secured which is subject to the information technology security of FI, such as the system configuration of the operation system and the security setting of the network devices.	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.	N/A
95.	**12.7 Capacity Management**		

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
96.	(1) To have the monitoring process, assessment of the competence and the information technology resources sufficiency of the Service Usage, Connection, or Access Information from the Third Party to be appropriate and continuous, together with reporting the result of such ongoing monitoring and assessment to the board of directors or the executives on regular basis for the readiness governance and the system sufficiency to support the continuity of business, including the consideration of risk reduction in a timely manner.	Google provides tools to help you manage your assets on our services. For example: • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Configuration Manager assists with: ○ Configure which users, groups, and other data to synchronize. ○ Set up rules to omit data, such as users or groups, from a sync. ○ Set up notifications and logging. • Admin Audit Logs - you can use the Admin audit log to see a record of actions performed in your Google Admin console. For example, you can see when an administrator added a user or turned on a Google Workspace service.	N/A
97.	(2) To stipulate the indicators, thresholds and triggers for information technology resource usage at each level and to set the processes of reporting and notification of the problems or the unusual event that occur during the Service Usage, Connection, or Access Information from the Third Party, guideline on coordination with the internal work units and external parties upon occurrence of an incident in compatible with the risk level and the materiality level of the service for FI's acknowledgement in a timely manner.	Refer to Row 96. 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 on our Status 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
98.	**12.8 Logging**		
99.	To ensure that the third party shall prepare the logging records which are sufficient and safe for FI's monitoring the access and the usage of the system or information of the users' footprint, including evidence of electronic transaction as required by law.	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service.	Data Security; (Cloud Data Processing Addendum)

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. The "Managing Google's Access to your Data" section of our Trusting your data with G Suite 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.	Ongoing Performance Monitoring
100.	**12.9 Security Monitoring**		
101.	(1) To ensure that the third party shall strictly, sufficiently and continuously monitor the system and threats, including that the material systems or services shall have scanning system to detect any unusual event that affecting the security of the system, network, and application, in order to be able to immediately cope with the threat.	Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. 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. 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:	Data Incidents; (Cloud Data Processing Addendum)

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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. 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: • Alert Center provides real-time actionable alerts and security insights about activity in your Google Workspace domain. • Cloud Identity is a unified identity, access app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximize end-user efficiency and protect your organization's data. • Security Center provides actionable security insights for Google Workspace to help protect your organisation.	
102.	(2) To arrange for the logging analysis of the systems/services that connect with the third party for protecting and monitoring threat.	Refer to Row 101.	N/A
103.	**12.10 Vulnerability Management and Penetration Testing**		
104.	(1) To ensure that the third party shall have the vulnerability management and penetration testing according to the generally accepted international standard and in consistent with the guideline policy of FI.	Vulnerability management Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring	Customer Penetration Testing

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Refer to our security whitepaper for more information. Penetration tests You can perform penetration testing of the Services at any time without Google's prior approval. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	
105.	(2) To audit the scopes and penetration test result of the third party to ensure that such test covering all systems that FI using service or connecting with Third party and the material threat.	Refer to Row 104.	N/A
106.	**12.11 Data Backup**		
107.	In case of FI using service or connecting with the third party that collect information of FI or consumers, FI shall have the standard practice relating to backup information for the third party to comply with the standard of FI which covers:		
108.	• Scopes/Details of data backup , and rounds of data backup	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
109.	• Method/Technology of data backup and data format	Refer to Row 108.	N/A
110.	• Duration on collection of data backup	Refer to Row 108.	N/A
111.	• To audit the accuracy of data backup	Refer to Row 108.	N/A
112.	• Process and method for recovering data	Refer to Row 108.	N/A
113.	• To audit the data backup (Restore)	Refer to Row 108.	N/A
114.	• Location of collecting of data backup	Refer to Row 108.	N/A
115.	**12.12 IT Incident Management**		

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
116.	(1) To set out duties and responsibilities of FI and the third party on management of any unusual information technology event, including to set the severity level of such unusual event and to inform FI upon the occurrence of such unusual event which relates to FI in an appropriate and timely manner.	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Status 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
117.	(2) If the unusual event affecting the business operation of FI in materiality, FI shall participate in remedial decisions to resolve the unusual event.	Refer to Row 116.	N/A
118.	(3) To require the third party to have the channel, system, or device for supporting in the case that FI detects and wish to report the information technology unusual event to the third party for acknowledgement so as to assist FI in monitoring the third party in resolving the unusual event that is relating to FI immediately.	Refer to Row 116.	N/A
119.	(4) To formally appoint a person to coordinate with FI in responding to the unusual event in relation to information technology.	This is a customer consideration.	N/A
120.	**12.13 Business Continuity Management**		
121.	(1) To have the business continuity management plan and the information technology emergency plan (the Disaster Recovery Plan) that cover Service Usage, Connection, or Access Information from the Third Party for supporting upon occurrence of events that may significantly affect the business continuity operation of FI.	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
122.	(2) The business continuity management plan and the disaster recovery plan shall take into account key factors or the risk that may occur or may cause suspension of Service Usage, Connection, or Access Information from the Third Party, the consequences on the business operation of FI and communications between the third party and FI, including problem or unusual event report to the board of directors or the executives immediately according to the severity level or consequence of the event.	Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including: -destruction of infrastructure required to provide the Services -interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures) -unavailability of key personnel	Business Continuity and Disaster Recovery

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		-emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) -pandemics	
123.	(3) To assess and test on the implementation of the business continuity management plan and the disaster recovery plan in order to be able to adopt, including the audit on the third party's plan, for consistency with the plan of FI, such as the consistency of scopes, definitions, and to specify the important time period: Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO).	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. 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.	Business Continuity and Disaster Recovery

Bank of Thailand
Announcement No. SorNorSor. 21/2562 Re: Criteria of Information Technology Risk Governance of Financial Institutions
Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
124.	(4) If FI is able to cooperatively test with the third party, FI shall attend the test in accordance with the business continuity management plan and the disaster recovery plan with the third party for assessing the readiness of the third party on recovering the system under the scopes of the MTPD, RTO, and RPO.	In addition to testing our own environments, Google also provides a number of tools and resources that enable firms to independently test their Google Cloud deployments. Our Disaster Recovery Scenarios for Data and Disaster Recovery for Applications articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively. You can also implement the following to help with your own testing: • Automate infrastructure provisioning with Deployment Manager. You can use Deployment Manager to automate the provisioning of VM instances and other Google Cloud infrastructure. If you're running your production environment on premises, make sure that you have a monitoring process that can start the disaster recovery process when it detects a failure and can trigger the appropriate recovery actions. • Monitor and debug your tests with Cloud Logging and Cloud Monitoring. Google Cloud has excellent logging and monitoring tools that you can access through API calls, allowing you to automate the deployment of recovery scenarios by reacting to metrics. When you're designing tests, make sure that you have appropriate monitoring and alerting in place that can trigger appropriate recovery actions.	N/A
125.	(5) Crisis Management Team of FI shall be aware of the third party's business continuity management plan and the disaster recovery plan for planning on the management in the related part.	Refer to Row 121.	N/A
126.	(6) To compile the problems which are found during the test of the business continuity management plan and the disaster recovery plan and to jointly improve with the third party.	Refer to Rows 121.	N/A