



# Bank of Thailand

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

### Google Cloud 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 Cloud 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 Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	<b>1. Risk Assessment from Service Usage, Connection, or Accessing Information from the Third Party</b>		
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 <a href="#">Board of Directors Handbook for Cloud Risk Governance</a> 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 <a href="#">Risk Governance of Digital Transformation in the Cloud</a> 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 recognizes that you need to plan and execute your migration carefully. Our <a href="#">Migration to Google Cloud</a> guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our <a href="#">How to put your company on a path to successful cloud migration whitepaper</a> provides guidance to help with the start of your digital transformation.  In addition, our <a href="#">Risk Assessment &amp; Critical Asset Discovery solution</a> evaluates your organization’s current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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 vulnerability which result in data loss or leakage, the third party's exercising excessive rights than permitted, and insufficient system resources.	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 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 <a href="#">security whitepaper</a> for more information.	N/A
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).	<p>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.</p> <p>Google will comply with all national data protection regulations applicable to it in the provision of the Services. This is addressed in the <a href="#">Cloud Data Processing Addendum</a>.</p>	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.	<p>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.</p> <ul style="list-style-type: none"> <li>Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our <a href="#">Global Locations page</a>.</li> <li>Information about the location of Google's subprocessors' facilities is available on our <a href="#">Google Cloud subprocessors page</a>.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>The same robust security measures apply to all Google facilities, regardless of country / region.</li> <li>Google makes the same commitments about all its subprocessors, regardless of country / region.</li> </ul> <p>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).</p>	<p>Data Transfers (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Data Security; Subprocessors (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Data Location (Service Specific Terms)</p>



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our <a href="#">Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper</a> .	
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
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.	<p>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 <a href="#">Engaging in a dialogue on customer controls and open cloud solutions blog post</a> and our <a href="#">Open Cloud page</a> for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk.</p> <p>To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the <a href="#">IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud</a>.</p> <p>In addition, 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:</p> <ul style="list-style-type: none"> <li>• <a href="#">Google Kubernetes Engine</a> is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</li> <li>• <a href="#">Migrate for Anthos</a> allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</li> <li>• 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 <a href="#">Compute Engine Documentation</a> page.</li> </ul>	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





# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> <li><a href="#">Google Cloud Operations</a> is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services.</li> <li><a href="#">Access Transparency</a> 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).</li> </ul> <p><u>Termination</u></p> <p>Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period.</p> <p>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.</p> <p><u>Information Security</u></p> <p>Refer to Row 21 for more information on Google's security measures.</p>	Term and Termination
14.	<b>2. Third Party Selection</b>		
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 in order to select the third party which is qualified in conformity with the objectives of FI in respect of its operation.	This is a customer consideration.	N/A
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 <a href="#">Board of Directors Handbook for Cloud Risk Governance</a> 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	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	
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.	<p><u>Financial status</u></p> <ul style="list-style-type: none"> <li>You can review Google's corporate and financial information on <a href="#">Alphabet's Investor Relations</a> 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.</li> <li>You can review Google's audited financial statements on <a href="#">Alphabet's Investor Relations</a> page.</li> </ul> <p><u>Reputation</u></p> <ul style="list-style-type: none"> <li>Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our <a href="#">Analyst Reports</a> page.</li> <li>Information about our referenceable customers is available on our <a href="#">Google Cloud Customer</a> page. In addition, our <a href="#">Financial Services Cloud Blog</a> and <a href="#">Financial Services solutions page</a> explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security &amp; compliance.</li> </ul> <p><u>Knowledge, experience and capability</u></p> <ul style="list-style-type: none"> <li>Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare &amp; life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our <a href="#">Choosing Google Cloud</a> page.</li> <li>You can review information about Google's historic performance of the services on our <a href="#">Google Cloud Status Dashboard</a>.</li> </ul>	N/A
19.	(2) Governance and organization culture of the third party.	You can review information about our mission, philosophies and culture on <a href="#">Alphabet's Investor Relations</a> page. It also provides information about our organisational policies e.g. our Code of Conduct.	N/A





# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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.</p> <p>More information is available at:</p> <ul style="list-style-type: none"><li>• Our <a href="#">infrastructure security</a> page</li><li>• Our <a href="#">security whitepaper</a></li><li>• Our <a href="#">cloud-native security whitepaper</a></li><li>• Our <a href="#">infrastructure security design overview</a> page</li><li>• Our <a href="#">security resources</a> page</li></ul> <p>In addition, you can review Google's <a href="#">SOC 2 report</a>.</p> <p><u>(2) Security of your data and applications in the cloud</u></p> <p>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.</p> <p>(a) <u>Security by default</u></p> <p>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:</p> <ul style="list-style-type: none"><li>• <u>Encryption at rest</u>. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud <a href="#">Encryption at rest</a> page.</li><li>• <u>Encryption in transit</u>. 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 <a href="#">Encryption in transit</a> page.</li></ul> <p>(b) <u>Security products</u></p>	



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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 <a href="#">Cloud Security Products</a> page.</p> <p>(c) <a href="#">Security resources</a></p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none"><li>• <a href="#">Security best practices</a></li><li>• <a href="#">Security use cases</a></li><li>• <a href="#">Security blueprints</a></li></ul>	
22.	(5) Business continuity management and readiness to cope with any threats or events.	<p>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.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our <a href="#">Disaster Recovery Planning Guide</a>.</p>	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.	<p>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.</p>	Representations and Warranties
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.	<p>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:</p> <ul style="list-style-type: none"><li>• <a href="#">ISO/IEC 27001:2013 (Information Security Management Systems)</a></li><li>• <a href="#">ISO/IEC 27017:2015 (Cloud Security)</a></li><li>• <a href="#">ISO/IEC 27018:2014 (Cloud Privacy)</a></li><li>• <a href="#">PCI DSS</a></li><li>• <a href="#">SOC 1</a></li><li>• <a href="#">SOC 2</a></li></ul>	Certifications and Audit Reports



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> <li><a href="#">SOC 3</a></li> </ul> <p>You can review Google's current <a href="#">certifications and audit reports</a> at any time. <a href="#">Compliance reports manager</a> provides you with easy, on-demand access to these critical compliance resources.</p>	
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.	<p>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.</p> <p>Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our <a href="#">Global Locations page</a>.</p> <p>Refer to our "<a href="#">Architecting disaster recovery for cloud infrastructure outages</a>" 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.</p>	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).	<p>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 <a href="#">Strengthening operational resilience in financial services by migrating to Google Cloud</a> whitepaper for more information.</p>	Data Export ( <a href="#">Cloud Data Processing Addendum</a> )
27.	<b>3. Preparation of Agreement or Terms on Service Usage, Connection, or Access Information from Third Party</b>		
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.	<p>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.</p>	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	<p>The Google Cloud services are described on our <a href="#">services summary</a> page.</p>	Definitions



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	
31.	(2) Roles, duties, and responsibilities of the third party and FI.	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks.</li> <li>• 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.</li> </ul> <p>Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our <a href="#">Cloud Security Alliance page</a> for more information on the allocations of responsibilities between Google and our customers.</p>	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 system and information (Integrity) and availability of information technology (Availability), and the standard on the consumer protection.	This is addressed in the <a href="#">Cloud Data Processing Addendum</a> where Google makes commitments to protect your data, including regarding security.	Data Security; Google's Security Measures ( <a href="#">Cloud Data Processing Addendum</a> )
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.	<p>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.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our <a href="#">Disaster Recovery Planning Guide</a>.</p>	<b>Business Continuity and Disaster Recovery</b>
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	<u>Monitoring</u>	





# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	as the change of owner, breach of security or confidentiality, and the third party being in the process of receivership, liquidation or insolvency.		
38.	(9) Guideline relating to dispute resolution and liability on damages.	<p><u>Dispute resolution</u></p> <p>Refer to your Google Cloud Financial Services Contract.</p> <p><u>Liability</u></p> <p>Refer to your Google Cloud Financial Services Contract.</p>	<p>Governing Law</p> <p>Liability</p>
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.	<p>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:</p> <ul style="list-style-type: none"> <li>• provide information about our subcontractors;</li> <li>• provide advance notice of changes to our subcontractors; and</li> </ul> <p>give regulated entities the ability to terminate if they have concerns about a new subcontractor.</p> <p>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.</p>	Google Subcontractors
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	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.	Data Transfers ( <a href="#">Cloud Data Processing Addendum</a> )



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	and obstructions may occur in the country where the third party is located or operates its business (Country Risk).	<ul style="list-style-type: none"> <li>Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our <a href="#">Global Locations page</a>.</li> <li>Information about the location of Google's subprocessors' facilities is available on our <a href="#">Google Cloud subprocessors page</a>.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>The same robust security measures apply to all Google facilities, regardless of country / region.</li> <li>Google makes the same commitments about all its subprocessors, regardless of country / region.</li> </ul> <p>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 <a href="#">Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper</a>.</p>	<p>Data Security; Subprocessors (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Data Location (Service Specific Terms)</p>
42.	<b>4. Monitoring of Performance of the Third Party</b>		
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.	<p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>The <a href="#">Status Dashboard</a> provides status information on the Services. <a href="#">Google Cloud Operations</a> is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud services.</li> <li><a href="#">Access Transparency</a> 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</li> </ul>	Ongoing Performance Monitoring



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
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.	<p>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 <a href="#">Incidents &amp; the Google Cloud dashboard</a> page.</p> <p>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 <a href="#">Data incident response whitepaper</a>.</p>	<p>Significant Developments</p> <p>Data Incidents (<a href="#">Cloud Data Processing Addendum</a>)</p>
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.	<p>Even before you are on Google Cloud, you can use our <a href="#">Risk Assessment &amp; Critical Asset Discovery solution</a> to evaluate your organization's current IT risk, identify where your critical assets reside, and receive recommendations for improving your security posture and resilience.</p> <p>Once on Google Cloud, you can leverage these tools to map and manage your cloud resources on an ongoing basis:</p> <ul style="list-style-type: none"> <li>• <a href="#">Google Cloud Operations</a> is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services.</li> <li>• <a href="#">Resource Manager</a> allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.</li> <li>• <a href="#">Cloud Deployment Manager</a> is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.</li> <li>• <a href="#">Risk Manager</a> enables you to receive reports on the controls that impact your overall security posture to remediate issues such as misconfigurations, helping to reduce risk and reduce time spent on managing security settings.</li> </ul>	N/A
46.	<b>5. Cancellation or Termination of Agreement or Terms</b>		



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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).	<p><u>Termination</u></p> <p>Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period.</p> <p>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.</p> <p><u>Transition</u></p> <p>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.</p> <p><u>Deletion</u></p> <p>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 <a href="#">Deletion on Google Cloud Platform whitepaper</a></p>	<p>Term and Termination</p> <p>Transition Term</p> <p>Deletion on Termination (<a href="#">Cloud Data Processing Addendum</a>)</p>
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.	<b>6. Information Technology Security on Service Usage, Connection, or Accessing Information from the Third Party</b>		



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
50.	<p>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 information technology security, and shall proceed with the following additional control practices:</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• <a href="#">ISO/IEC 27001:2013 (Information Security Management Systems)</a></li> <li>• <a href="#">ISO/IEC 27017:2015 (Cloud Security)</a></li> <li>• <a href="#">ISO/IEC 27018:2014 (Cloud Privacy)</a></li> <li>• <a href="#">PCIDSS</a></li> <li>• <a href="#">SOC 1</a></li> <li>• <a href="#">SOC 2</a></li> <li>• <a href="#">SOC 3</a></li> </ul> <p>You can review Google's current <a href="#">certifications and audit reports</a> at any time. <a href="#">Compliance reports manager</a> provides you with easy, on-demand access to these critical compliance resources.</p> <p>For information on Google's security measures and certifications refer to Row 21.</p>	<p>Certifications and Audit Reports</p>
51.	<p><b>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.</b></p>		
52.	<p>(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.</p>	<p>You can leverage these tools to map and manage your cloud resources on an ongoing basis:</p> <ul style="list-style-type: none"> <li>• <a href="#">Google Cloud Operations</a> is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud services, including availability and uptime of the services.</li> <li>• <a href="#">Resource Manager</a> allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.</li> <li>• <a href="#">Cloud Deployment Manager</a> is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.</li> </ul>	<p>N/A</p>



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> <li><a href="#">Risk Manager</a> enables you to receive reports on the controls that impact your overall security posture to remediate issues such as misconfigurations, helping to reduce risk and reduce time spent on managing security settings.</li> </ul>	
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.	<ul style="list-style-type: none"> <li>Name of the Third party</li> </ul>	Refer to our <a href="#">Google Contracting Entity page</a> for information about which Google entity is the provider of the services in each country.	N/A
55.	<ul style="list-style-type: none"> <li>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.</li> </ul>	Refer to Row 54.	N/A
56.	<ul style="list-style-type: none"> <li>Name of service/work system</li> </ul>	Google Cloud is a public cloud service. It provides Infrastructure as a Service and Platform as a Service. Customers can choose to deploy Google Cloud as part of a hybrid or multi-cloud deployment.	N/A
57.	<ul style="list-style-type: none"> <li>Characteristics and scope of work</li> </ul>	The Google Cloud services are described on our <a href="#">services summary</a> 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.	<ul style="list-style-type: none"> <li>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.</li> </ul>	Refer to Rows 56 and 57.	N/A
59.	<ul style="list-style-type: none"> <li>Risk level and material risk of Service Usage, Connection, or Access Information from the Third Party</li> </ul>	This is a customer consideration.	N/A
60.	<ul style="list-style-type: none"> <li>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.</li> </ul>	<p>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.</p> <ul style="list-style-type: none"> <li>Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our <a href="#">Global Locations page</a>.</li> <li>Information about the location of Google's subprocessors' facilities is available on our <a href="#">Google Cloud subprocessors page</a>.</li> </ul> <p>Google provides the same contractual commitments and technical and organizational</p>	<p>Data Transfers (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Data Security; Subprocessors (<a href="#">Cloud Data</a>)</p>



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>measures for your data regardless of the country / region where it is located. In particular:</p> <ul style="list-style-type: none"> <li>• The same robust security measures apply to all Google facilities, regardless of country / region.</li> <li>• Google makes the same commitments about all its subprocessors, regardless of country / region.</li> </ul> <p>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).</p> <p>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our <a href="#">Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper</a>.</p>	<p><a href="#">Processing Addendum</a>)</p> <p>Data Location (Service Specific Terms)</p>
61.	<ul style="list-style-type: none"> <li>• Commencement date and termination date of the agreements or the terms of Service Usage, Connection, or Access Information from the Third Party.</li> </ul>	Refer to your Google Cloud Financial Services Contract.	Term and Termination
62.	<ul style="list-style-type: none"> <li>• Certificates in accordance with the related international standard regarding information technology (if any).</li> </ul>	<p>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:</p> <ul style="list-style-type: none"> <li>• <a href="#">ISO/IEC 27001:2013 (Information Security Management Systems)</a></li> <li>• <a href="#">ISO/IEC 27017:2015 (Cloud Security)</a></li> <li>• <a href="#">ISO/IEC 27018:2014 (Cloud Privacy)</a></li> <li>• <a href="#">PCI DSS</a></li> <li>• <a href="#">SOC 1</a></li> <li>• <a href="#">SOC 2</a></li> <li>• <a href="#">SOC 3</a></li> </ul> <p>You can review Google's current <a href="#">certifications and audit reports</a> at any time. <a href="#">Compliance reports manager</a> provides you with easy, on-demand access to these critical compliance resources.</p>	Certifications and Audit Reports



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
63.	<ul style="list-style-type: none"> <li>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.</li> </ul>	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.	<b>12.2 Information Security</b>		
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.	<p>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. Refer to our <a href="#">Choosing an Encryption Option page</a> for help to identify the solutions that best fit your requirements for key generation, storage, and rotation.</p> <p><u>Data at endpoint</u></p> <p>Google provides customers with tools that facilitate <a href="#">ubiquitous data encryption</a> which delivers unified control over data at-rest, in-use, and in-transit, all with keys that are under your control.</p> <p><u>Data in transit</u></p> <p>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 <a href="#">Encryption in transit</a> page.</p> <p><u>Data at rest</u></p> <p>Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud <a href="#">Encryption at rest</a> page.</p>	Data Security; Google's Security Measures ( <a href="#">Cloud Data Processing Addendum</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 Cryptographic Keys), including creation, collection, usage, backing up, revocation, and renewal of cryptographic keys	<p>You can choose to use these encryption and key management tools provided by Google:</p> <ul style="list-style-type: none"> <li><a href="#">Cloud KMS</a> is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises.</li> </ul>	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> <li>• <a href="#">Cloud HSM</a> 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.</li> <li>• Customer-managed encryption keys for <a href="#">Cloud SQL</a> and <a href="#">GKE persistent disks</a>.</li> <li>• <a href="#">Cloud External Key Manager</a> 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.</li> <li>• <a href="#">Key Access Justification</a> 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.</li> </ul>	
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.	<ul style="list-style-type: none"> <li>• Category of cryptographic keys.</li> </ul>	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
69.	<ul style="list-style-type: none"> <li>• Details of the system, including the control process of the information encryption on each processes along with the lifecycle management of cryptographic keys.</li> </ul>	Refer to Rows 65 and 66 for more information on Google's encryption features.	N/A
70.	<ul style="list-style-type: none"> <li>• Suggestion on use and control of encrypting information.</li> </ul>	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 Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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.	<p>There are a number of ways to perform effective access / configuration management using the services:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cloud Identity and Access Management</a> helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources.</li> <li>• <a href="#">Resource Manager</a> allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.</li> <li>• <a href="#">Cloud Deployment Manager</a> is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.</li> <li>• <a href="#">Assured Workloads</a> helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints.</li> </ul>	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.	<p>Our <a href="#">Risk and Compliance as Code (RCaC) Solution</a> 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.</p> <p>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.</p> <p>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.</p>	<p>N/A</p> <p>Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (<a href="#">Cloud Data Processing Addendum</a>)</p>
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



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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.	<ul style="list-style-type: none"> <li>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.</li> </ul>	Refer to Row 74-77 for information on access management.	N/A
81.	<ul style="list-style-type: none"> <li>To identify the user by two-factor authentication and to have connection through virtual private network (VPN).</li> </ul>	Refer to Row 74-77 for information on access management.	N/A
82.	<ul style="list-style-type: none"> <li>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.</li> </ul>	Refer to Row 74-77 for information on access management.	N/A
83.	<ul style="list-style-type: none"> <li>To be able to specify and to audit the source of devices or system which remotely connect with the system of FI.</li> </ul>	Refer to Row 74-77 for information on access management.	N/A
84.	<ul style="list-style-type: none"> <li>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.</li> </ul>	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.	<b>12.4 Communication Security</b>		
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. More information is available on the Google Cloud <a href="#">Encryption in transit</a> page.	Data Security; Security Measures ( <a href="#">Cloud Data Processing Addendum</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	At Google we rely on a zero trust system known as <a href="#">BeyondCorp</a> , to move beyond the idea of a privileged corporate network. For more information on our zero trust approach refer to our <a href="#">What is Zero Trust Identity Security?</a> blog post.	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	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.	<p>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.</p> <p>Our <a href="#">Autonomic Security Operations (ASO) solution</a>:</p> <ul style="list-style-type: none"> <li>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.</li> <li>enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution.</li> </ul> <p>Information on Google's security products is available <a href="#">here</a>. Here are some examples:</p> <ul style="list-style-type: none"> <li><a href="#">Cloud Security Scanner</a> automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities.</li> <li><a href="#">Event Threat Detection</a> automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment.</li> <li><a href="#">Cloud Security Command Center and Security Health Analytics</a> provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.</li> </ul>	
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.	Security Measures; Data Storage, Isolation and Logging ( <a href="#">Cloud Data Processing Addendum</a> )
90.	<b>12.5 Change Management</b>		
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.	Changes to Services



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>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.</p> <p>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.</p> <p>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.</p>	
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.	<b>12.6 System Configuration Management</b>		
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.	<p>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.</p> <p>There are a number of ways to perform effective configuration management using the services:</p> <ul style="list-style-type: none"><li>• Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources.</li><li>• Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.</li><li>• Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.</li></ul>	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"> <li>Assured Workloads helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints.</li> </ul>	
95.	<b>12.7 Capacity Management</b>		
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.	<p>Google provides tools to help you manage your assets on our services. For example:</p> <p><a href="#">Cloud Asset Inventory</a> allows you to view, monitor, and analyze all your Google Cloud and Anthos assets across projects and services. Not only can you export a snapshot of your entire inventory at any point of time, you can also get real-time notifications on asset config changes.</p> <p><a href="#">Cloud Data Loss Prevention</a> helps classify your data on or off cloud giving you the insights you need to ensure proper governance, control, and compliance.</p> <p><a href="#">Resource Manager</a> allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.</p> <p><a href="#">Cloud Deployment Manager</a> is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.</p>	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.	<p>Refer to Row 96.</p> <p>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.</p> <p>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 <a href="#">Incidents &amp; the Google Cloud dashboard</a> page.</p>	<p>Significant Developments</p> <p>Data Incidents (<a href="#">Cloud Data Processing Addendum</a>)</p>



# Bank of Thailand

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

### Google Cloud Platform 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 <a href="#">Data incident response whitepaper</a> .	
98.	<b>12.8 Logging</b>		
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.	<p>Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.</p> <ul style="list-style-type: none"> <li>• <a href="#">Cloud Identity and Access Management</a> helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources.</li> <li>• <a href="#">Cloud Audit Logs</a> help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events.</li> <li>• <a href="#">Multi-Factor Authentication</a> provides a wide variety of verification methods to help protect your user accounts and data.</li> </ul> <p>The "Managing Google's Access to your Data" section of our <a href="#">Trusting your data with Google Cloud whitepaper</a> explains Google's data access processes and policies.</p> <p>In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools:</p> <ul style="list-style-type: none"> <li>• <a href="#">Access Transparency</a> 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).</li> <li>• <a href="#">Access Approval</a> 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.</li> </ul>	<p>Data Security; Additional Security Controls (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (<a href="#">Cloud Data Processing Addendum</a>)</p>



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
100.	<b>12.9 Security Monitoring</b>		
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.	<p>Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents.</p> <p>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 <a href="#">Data incident response whitepaper</a>.</p> <p>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.</p> <p>Our <a href="#">Autonomic Security Operations (ASO) solution</a>:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution.</li></ul> <p>Information on Google's security products is available <a href="#">here</a>. Here are some examples:</p> <ul style="list-style-type: none"><li>• <a href="#">Cloud Security Scanner</a> automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities.</li><li>• <a href="#">Event Threat Detection</a> automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment.</li><li>• <a href="#">Cloud Security Command Center and Security Health Analytics</a> provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems.</li></ul>	Data Incidents ( <a href="#">Cloud Data Processing Addendum</a> )



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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.	<b>12.10 Vulnerability Management and Penetration Testing</b>		
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.	<p><u>Vulnerability management</u></p> <p>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 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 <a href="#">security whitepaper</a> for more information.</p> <p><u>Penetration tests</u></p> <p>You can perform penetration testing of the Services at any time without Google's prior approval.</p> <p>In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available <a href="#">here</a>.</p>	Customer Penetration Testing
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.	<b>12.11 Data Backup</b>		
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.	<ul style="list-style-type: none"> <li>Scopes/Details of data backup , and rounds of data backup</li> </ul>	Regulated entities can use <a href="#">Cloud Storage</a> as part of their backup routine. Refer to our <a href="#">Disaster Recovery Building Blocks</a> and <a href="#">Disaster Recovery Scenarios for Data</a> articles for more information about how you can use the services for data backup.	N/A
109.	<ul style="list-style-type: none"> <li>Method/Technology of data backup and data format</li> </ul>	Refer to Row 108.	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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.	<b>12.12 IT Incident Management</b>		
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 <a href="#">Incidents &amp; the Google Cloud dashboard</a> 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 <a href="#">Data incident response whitepaper</a> .	Significant Developments  Data Incidents ( <a href="#">Cloud Data Processing Addendum</a> )
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.	<b>12.13 Business Continuity Management</b>		
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 <a href="#">Disaster Recovery Planning Guide</a> .	Business Continuity and Disaster Recovery



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
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: <ul style="list-style-type: none"><li>-destruction of infrastructure required to provide the Services</li><li>-interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures)</li><li>-unavailability of key personnel</li><li>-emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake)</li><li>-pandemics</li></ul>	Business Continuity and Disaster Recovery
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 <a href="#">Google Cloud Architecture Framework</a> . We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our <a href="#">Architecting disaster recovery for cloud infrastructure outages</a> 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 <a href="#">article</a> we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud.	Business Continuity and Disaster Recovery
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 <a href="#">Disaster Recovery Scenarios for Data</a> and <a href="#">Disaster Recovery for Applications</a> articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively.	N/A



# Bank of Thailand

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

### Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>You can also implement the following to help with your own testing:</p> <ul style="list-style-type: none"><li>Automate infrastructure provisioning with Deployment Manager. You can use <a href="#">Deployment Manager</a> 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.</li><li>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.</li></ul>	
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