



FISC Security Guidelines 9th edition (revised March 2020)

Google Workspace Mapping

This document is designed to help financial institutions supervised by the Financial Services Agency of Japan (“**regulated entity**”) to consider the FISC Security Guidelines on Computer Systems for Financial Institutions 9th edition (revised March 2020) (“**framework**”) in the context of Google Workspace and the Google Cloud Financial Services Contract.

In this document, we focus on Guideline 21 about contract requirements. 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. Regulated entities should use the table below together with the 9th edition (revised March 2020) of the framework [available from FISC](#).

If you would like to understand how our control environment aligns with the FISC Security Guideline more broadly, you can request the Google Cloud FISC handbook via your Google Cloud account representative.

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	C21	Google concludes the Google Cloud Financial Services Contract with regulated entities.	N/A
2	1.	The Google Cloud Financial Services Contract addresses each of the items in the framework. To assist you, we’ve provided information for each of the areas you need to consider in the rows that follow. <u>Changes to contract</u> For more information on changes to the contract refer to Row 9. For more information on changes to the service refer to Row 10.	N/A N/A
3	1. (1) Basic provisions		
4	1.(1),1)	The roles and responsibilities of the parties, definition of terms, and governing law are set out in the Google Cloud Financial Services Contract. Damages are also addressed in the Google Cloud Financial Services Contract. In particular, if Google’s performance of the Services does not meet the Google Workspace Service Level Agreement regulated entities may claim service credits.	Definitions; Liability; Governing Law Services
5	1.(1), 2)	N/A	N/A
6	1.(1), 3)	<u>Quality</u> You can monitor Google’s performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. <u>Verification</u> 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: <ul style="list-style-type: none"> • 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.	Ongoing Performance Monitoring Certifications and Audit Reports



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
7	1.(1), 4)	<p><u>Working hours</u></p> <p>The SLAs contain Google’s commitments regarding availability of the Services. They are available on the Google Workspace Service Level Agreement page.</p> <p><u>Accessible locations</u></p> <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"> Information about the location of Google’s facilities is available here. Information about the location of Google’s subprocessors’ facilities is available here. <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"> 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. <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 Trusting your data with Google Workspace whitepaper.</p>	<p>Services</p> <p>Data Location (Service Specific Terms)</p> <p>Data Security; Subprocessors (Data Processing Amendment)</p> <p>Data Transfers (Data Processing Amendment)</p>
8	1.(1), 5)	Refer to your Google Cloud Financial Services Contract.	Use Restrictions
9	1.(1), 6)	As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Beyond these limited updates, any contract changes must be made in writing and signed by both parties.	Changes to Terms; Amendments
10	1.(1), 7)	<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>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.</p>	Changes to Services
11	1. (2)	<p><u>Service specifications</u></p> <p>The Google Workspace services are described on our services summary page.</p>	Definitions



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p><u>Data protection</u></p> <p>This is addressed in the Data Processing Amendment where Google makes commitments to protect your data, including regarding security, use, incidents, access and retention.</p>	Data Security; Security Measures (Data Processing Amendment)
12	1.(2), 1)	<p><u>Fees</u></p> <p>Refer to your Google Cloud Financial Services Contract.</p> <p><u>Expiry</u></p> <p>Refer to your Google Cloud Financial Services Contract.</p>	Payment Terms Term and Termination
13	1.(2), 2)	Refer to Row 11 for a description of the Google Workspace services. The customer decides which services to use, how to use them and for what purpose. Therefore the customer stays in control of the relevant activities.	N/A
14	1.(2), 3)	Refer to Row 11 for a description of the Google Workspace services and Row 10 on service modifications.	N/A
15	1.(2), 4)	Refer to your Google Cloud Financial Services Contract.	Confidentiality
16	1.(2), 5)	Google will ensure its employees comply with Google's security measures and that all personnel authorized to process customer data are under an obligation of confidentiality.	Data Security; Security Compliance by Google Staff (Data Processing Amendment)
17	1.(2), 6)	<p>The security of a cloud service consists of two key elements:</p> <p><u>(1) Security of Google's infrastructure</u></p> <p>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.</p> <p>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.</p> <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">• Our infrastructure security page• Our security whitepaper• Our cloud-native security whitepaper• Our infrastructure security design overview page• Our security resources page	Data Security; Security Measures (Data Processing Amendment)



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>In addition, you can review Google's SOC 2 report.</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><u>(a) 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"> • Encryption at rest. Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. • Encryption in transit. Google encrypts all data while it is "in transit"—traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. <p><u>(b) Security products</u></p> <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 Cloud Security Products page.</p> <p><u>(c) Security resources</u></p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none"> • Security best practices • Security use cases 	
18	1.(2), 7)	Regulated entities can use Spinbackup as part of their backup routine. Refer to our solutions page for more information about how you can configure Spinbackup Google Workspace backup and restore your Google Workspace data.	Customer's Security Responsibilities
19	1. (3)	<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>If Google's performance of the Services does not meet the Google Workspace Service Level Agreement regulated entities may claim service credits.</p>	<p>Ongoing Performance Monitoring</p> <p>Services</p>
20	1. (4)	<u>Information</u>	



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		<p>Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.</p> <p><u>Cooperation with supervisory authorities</u></p> <p>Google grants audit, access and information rights to supervisory authorities and their appointees. This includes access to both documentation and information and the right to conduct onsite visits.</p> <p>Google will fully cooperate with supervisory authorities exercising their audit, information and access rights.</p> <p><u>Reporting, communication and Incident Response</u></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 on our Status Dashboard 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 Data incident response whitepaper.</p>	<p>Protection of Customer Data</p> <p>Regulator Information, Audit and Access</p> <p>Enabling Customer Compliance</p> <p>Significant Developments</p> <p>Data Incidents (Data Processing Amendment)</p>
21	1.(4), 1)	<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">• 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).	<p>Ongoing Performance Monitoring</p>
22	1.(4),2)	<p>Regulated entities can use the following functionality to control the Services:</p> <ul style="list-style-type: none">• Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources.	<p>Google's Compliance with Instructions (Data Processing Amendment)</p>
23	1.(4),3)	<p>Refer to your Google Cloud Financial Services Contract.</p>	<p>Governing Law</p>



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24	1.(4),4)	In addition to the support services described on our technical support services guidelines page, Google provides documentation to explain how regulated entities and their employees can use our services. Information on the reliability of the Services is available on our Google Cloud Help page. If a regulated entity would like more guided training, Google also provides a variety of courses and certifications .	Technical Support
25	1.(4),5)	For more information on business continuity refer to Row 28.	Business Continuity and Disaster Recovery
26	1.(4),6)	For more information on Google's process for reporting incidents refer to Row 20.	N/A
27	1.(4),7)	For more information on Google's process for reporting incidents refer to Row 20. 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 particular, Cloud Audit Logs help your security teams maintain audit trails in Google Workspace and view detailed information about Admin activity, data access, and system events.	N/A
28	1.(4),8)	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. Information on the reliability of the Services is available on our Google Cloud Help page	Business Continuity and Disaster Recovery
29	1. (5)	Google will comply with all laws and regulations applicable to it in the provision of the Services. 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.	Representations and Warranties
30	1. (6)	<u>Termination</u> Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law. In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency. <u>Deletion</u> On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. <u>Transition assistance</u>	Term and Termination Deletion on Termination (Data Processing Amendment)



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		For more information on how Google can assist on transition of the service to another service provider or back to the regulated entity refer to Row 33.	N/A
31	1.(6), 1)	For more information on the regulated entity's ability to terminate the contract refer to Row 30.	N/A
32	1.(6), 2)	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 (Data Processing Amendment)
33	1.(6), 3)	<p>Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). 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>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.</p> <p>In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.</p>	<p>Transition Term</p> <p>Transition Assistance</p> <p>Data Export (Data Processing Amendment)</p>
34	1. (7)	Refer to your Google Cloud Financial Services Contract.	Liability
35	1. (8)	<p>You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications.</p> <p>Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.</p>	<p>Intellectual Property</p> <p>Protection of Customer Data</p>
36	1. (9)		
37	1. (9), 1)	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Protection of Customer Data; Confidentiality
38	1. (9), 2)	For more information on Google's reporting, communication and incident response refer to Row 20.	N/A
39	1. (10) Outsourcing to		



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	multiple contractors		
40	1. (10)	This is a customer consideration	N/A
41	1. (11) Management of subcontractors		
42		<p>Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support.</p> <p>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"> • 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. <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.</p> <p>Before engaging a subcontractor, Google will conduct an assessment considering the risks related to subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.</p>	Google Subcontractors
43	1. (11), 2)	Google will remain accountable to you for the performance of all subcontracted obligations.	Google Subcontractors
44	1. (11), 3)	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, and security requirements).	Google Subcontractors
45	1. (11), 4)	Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors
46	1. (12) Audit and		



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	monitoring		
47	1. (12), 1)	Google grants audit, access and information rights to regulated entities, supervisory authorities and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
48	1. (12), 2)	Google is committed to supporting regulated entities with audits or examinations of our services. As this support is not included in our usual publicly listed service fees, Google may charge an additional fee in connection with an audit or examination. Google will provide further details of any fee in advance of the activity when the scope of the activity is known.	Enabling Customer Compliance; Fees
49	1. (12), 3)	Google is committed to supporting regulated entities with audits or examinations of our services and will fully cooperate with regulated entities exercising their audit, information and access rights.	Enabling Customer Compliance
50	1. (13)		
51	1. (13), 1)	Google grants audit, access and information rights to regulated entities and their appointees. This includes access to both documentation and information and the right to conduct onsite visits.	Customer Information, Audit and Access
52	1. (13), 2)	Prior discussions about scope will enable Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it does not create undue risk to your environment or that of any other Google customer.	Arrangements
53	1. (13), 3)	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access. For more information on site visits and prior discussion refer to Row 52.	N/A
54	1. (14) Failure and replacement of storage devices		
55	1. (14)	For more information about deletion, including secure decommissioning when physical storage media reaches the end of its life-cycle refer to our Deletion on Google Workspace Trust whitepaper .	Data Deletion (Data Processing Amendment)
56	1. (15) Precautions related to failure support contracts abroad		



FISC Security Guidelines

Google Workspace Mapping

#	Reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
57	1. (15)	Our support services are available in Japanese language. For more information about our language support refer to our Language Support page .	Technical Support
58	1. (16) Ensuring traceability		
59	1. (16)	For more information on Google's reporting, communication and data incident response refer to Row 20. For more information about traceability refer to Row 27.	N/A
60	2.	The SLAs contain Google commitments regarding availability of the Service. They are available on the Google Workspace Service Level Agreement page. The technical support services guidelines describe our support response times.	Services Technical Support
61	3.	Information on the reliability of the Services is available on our Google Cloud Help page.	N/A
62	3. (1)	For more information on data extraction and Google's cooperation with the data migration process refer to Row 33.	N/A
63	3. (2)	For more information on data extraction refer to Row 33. The cost of migration is transparent and based on our publicly listed service fees. Our services enable you to transfer your data independently. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services subject to agreeing additional fees.	Transition Assistance
64	3. (2)	For more information on security refer to Row 17.	N/A