FISC Security Guidelines 14th Edition (revised March 2026)

Handbook for Google Cloud and Google Workspace

This document provides an overview of the security management measures implemented by Google Cloud and Google Workspace as a part of the information disclosure requirement under “FISC Security Guideline 14th Edition (revised March 2026)” required by FISC. Google's controls described in this document are certified by the third-party audit compliance programs ISO / IEC 27001, ISO / IEC 27017, ISO / IEC 27018, and ISO/IEC 42001. This handbook explains how customers confirm Google Cloud services and related compliance programs ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 42001 so that they can meet the requirements.

Control number is compliant with the FISC guidelines. Items to be implemented within the scope of customer's responsibility are described as "-".

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
C1	-	-
C1-1	-	-
C1-2	To assist you, Google provides the following reference information for managing Third Party risks including cybersecurity risks. Reference information： Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world. Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	-
C2	-	-
C3	-	-
C4	To assist you, Google provides the following reference information to help you establish a security management system for outsourcing / cloud adoption. Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	-
C4-1	-	-
C4-2	-	-
C5-1	Google provides tools to help you manage your assets on our services. For example: Google Cloud: Cloud Asset Inventory 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. Cloud Data Loss Prevention helps classify your data on or off cloud giving you the insights you need to ensure proper governance, control, and compliance. Resource Manager allows you to programmatically manage Google Cloud container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud resources."Google provides tools to help you manage your assets on our services. Mandiant Attack Surface Management (ASM) allows you to discover and analyze your internet assets across today’s dynamic, distributed, and shared environments, while continually monitoring the external ecosystem for exploitable exposures. Workspace: Admin Console allows you to add users, manage devices and configure security and settings. Security center provides advanced security information and analytics, and added visibility and control into security issues affecting your domain. Endpoint allows you to manage devices used in your organization to keep work content safe on personal and company-owned devices.	-
C5-2	To assist you, Google provides the following reference information to help you collecting threat and vulnerability information.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google publishes Threat Horizons intelligence reports to help keep your organization on top of the latest developments in the security landscape: https://cloud.google.com/solutions/security/leaders?e=0&hl=en#latest-threat-intelligence-from-google-experts Google publishes bulletins that contain public security updates, vulnerabilities and known issues for certain Google Cloud services, via https://cloud.google.com/support/bulletins.	
C5-3	To assist you, we provide the following information regarding Google's vulnerability management practices to serve as a reference for customers when managing vulnerability responses for systems owned by third parties. Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information. Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum) Certifications and Audit Reports
C5-4	-	-
C5-5	All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Refer to our security whitepaper for more information.	-
C6	-	-
C7	-	-
C8	-	-
C9	-	-
C10	-	-
C11	-	-
C12	-	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
C13	-	-
C14	-	-
C15	To assist you, Google provides documentation for Google Cloud and Workspace to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	-
C16	-	-
C17	-	-
C18	-	-
C19	-	-
C20	It is the customer's responsibility to conduct an appropriate evaluation when selecting a cloud provider. 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. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page. ◯ Compliance Google Cloud Compliance https://cloud.google.com/security/compliance Latest Compliance Offerings https://cloud.google.com/security/compliance/offerings ◯ Google Cloud Terms of Service Overview of Google Cloud Platform Services https://cloud.google.com/terms/services Google Cloud Platform Service Level Agreements https://cloud.google.com/terms/sla/ Overview of Google Workspace https://workspace.google.co.jp/intl/ja/terms/user_features.html Google Workspace Service Level Agreements https://workspace.google.com/terms/sla.html	-
C20 (cont.)	Google Cloud Service-Specific Terms https://cloud.google.com/terms/service-terms Google Workspace Service-Specific Terms https://workspace.google.co.jp/intl/ja/terms/service-terms/index.html Data Processing and Security Terms	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	https://cloud.google.com/terms/data-processing-terms#top_of_page Cloud Data Processing Addendum https://cloud.google.com/terms/data-processing-addendum#top_of_page Google Cloud Subprocessors https://cloud.google.com/terms/subprocessors Google Workspace and Cloud Identity Subprocessors https://workspace.google.com/terms/subprocessors.html Technical Support Services Guidelines https://cloud.google.com/terms/tssg/ ◯Google Cloud Security Google Security Whitepaper https://cloud.google.com/security/overview/whitepaper Cloud-Native Security Whitepaper https://cloud.google.com/security/beyondprod Google Workspace Security Whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Infrastructure Security https://cloud.google.com/security/infrastructure/ Infrastructure Security Design Overview https://cloud.google.com/security/infrastructure/design/ An Overview of Google's Commitment to Secure by Design https://publicpolicy.google/resources/google_commitment_secure_by_design_overview.pdf Security Resources https://cloud.google.com/security Cloud Security Products https://cloud.google.com/products/security-and-identity Google Cloud security best practices center https://cloud.google.com/security/best-practices Security Use Cases https://cloud.google.com/security/showcase/	
C20 (cont.)	◯ Google Cloud Locations Google Cloud Locations https://cloud.google.com/about/locations/	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google Cloud Whitepaper on Data Residency, Operational Transparency, and Customer Privacy https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf ◯ Google Cloud Disaster Recovery and Incident Management Disaster Recovery Planning Guide https://cloud.google.com/architecture/dr-scenarios-planning-guide Google Cloud Service Health Dashboard https://status.cloud.google.com/ Personalized Service Health https://cloud.google.com/service-health Cloud Monitoring https://cloud.google.com/monitoring Data Incident Response Whitepaper https://cloud.google.com/docs/security/incident-response ◯ Data Deletion Data Deletion on the Google Cloud Platform Whitepaper https://cloud.google.com/security/deletion ◯ Support Google Cloud Support https://cloud.google.com/support-hub Language Support https://cloud.google.com/support/docs/language-working-hours ◯ Corporate Information Alphabet Investor Relations https://abc.xyz/investor/	
C21	Google concludes the Google Cloud Financial Services Contract with regulated entities.	-
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. Changes to contract For more information on changes to the contract refer to 1.(1), 6). For more information on changes to the service refer to 1.(1), 7).	-
1. (1)	-	-
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.	Definitions; Liability; Governing Law

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Damages are also addressed in the Google Cloud Financial Services Contract. In particular, if Google's performance of the Services does not meet the Service Level Agreements regulated entities may claim service credits. Google Cloud Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreements https://workspace.google.com/terms/sla/ The governing law can be set as Japanese law, and the court of jurisdiction can be set as the Tokyo District Court.	Services
1.(1), 2)	-	-
1.(1), 3)	Quality You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. Verification Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Ongoing Performance Monitoring Certifications and Audit Reports
1.(1), 4)	Working hours The SLAs contain Google's commitments regarding availability of the Services. They are available on the Service Level Agreements page. The support services are described on our Technical Support Services Guidelines page. This includes hours of operation, response times and languages supported. Accessible locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page.	Services Technical Support Data Location (Google Cloud Service Specific Terms) Google Workspace Service Specific Terms

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: The same robust security measures apply to all Google facilities, regardless of country / region. Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. Google Cloud Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreements https://workspace.google.com/terms/sla.html Google Cloud Services: Technical Support Services Guidelines https://cloud.google.com/terms/tssg/ Google Workspace Technical Support Services Guidelines https://workspace.google.com/terms/tssg/ Global Locations https://cloud.google.com/about/locations/ Google Cloud subprocessors https://cloud.google.com/terms/subprocessors Google Workspace and Cloud Identity Subprocessors https://workspace.google.com/intl/en/terms/subprocessors.html Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf	Data Security; Subprocessors (Cloud Data Processing Addendum) Data Transfers (Cloud Data Processing Addendum)
1.(1), 5)	Refer to your Google Cloud Financial Services Contract.	Use Restrictions
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
1.(1), 7)	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also control changes to your use of the services. Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services.	Changes to Services

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period. You can learn more about Google Cloud's approach to change management at https://cloud.google.com/docs/cloud-approach-to-change	
1. (2)	Service specifications The Google Cloud services are described on our services summary page. The Google Workspace services are described on our services summary page. Data protection This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. Google Cloud Platform Services Summary https://cloud.google.com/terms/services Google Workspace Services Summary https://workspace.google.com/terms/user_features Cloud Data Processing Addendum https://cloud.google.com/terms/data-processing-addendum	Definitions Confidentiality Data Security; Google's Security Measures; (Cloud Data Processing Addendum)
1.(2), 1)	Fees Refer to your Google Cloud Financial Services Contract. Expiry Refer to your Google Cloud Financial Services Contract.	Payment Terms Term and Termination
1.(2), 2)	Refer to 1. (2) for a description of the Google Cloud services. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement. Google recognizes that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers. It is important for regulated entities to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organization and the cloud service provider. Responsibility in the cloud is assigned as follows: Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.(2), 3)	Refer to 1. (2) for a description of the Google Cloud services and 1.(1), 7) on service modifications.	-
1.(2), 4)	Refer to your Google Cloud Financial Services Contract. Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.	Confidentiality
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. Trusted infrastructure https://cloud.google.com/security/infrastructure	Data Security; Access and Compliance (Cloud Data Processing Addendum)
1.(2), 6)	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and security of information when using a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: Our infrastructure security page Our security whitepaper Our cloud-native security whitepaper Our infrastructure security design overview page Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you:	Confidentiality Data Security; Google's Security Measures; (Cloud Data Processing Addendum)

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: Google Cloud security best practices center	
1.(2), 7)	For Google Cloud, you can use Google Cloud Back Up and Disaster Recovery to manage backups. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. For Google Workspace, you can export their entire organization's data using Data Export. Google also has many tools that you can use to work with and extract your organization's Google Workspace data, such as APIs and BigQuery or partner solutions, such as Afi and SpinOne. For additional third-party and partner options, you can also check out our Google Cloud directory.	-
1. (3)	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. If Google's performance of the Services does not meet the Google Cloud Service Level Agreements regulated entities may claim service credits. Google Cloud Platform Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreement https://workspace.google.com/terms/sla	Ongoing Performance Monitoring Services
1. (4)	Information 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. Cooperation with supervisory authorities 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. Google will fully cooperate with supervisory authorities exercising their audit, information and access rights. Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights. Reporting, communication and Incident Response	Protection of Customer Data Regulator Information, Audit and Access Enabling Customer Compliance Significant Developments

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
1.(4), 1)	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: The Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud's Observability is an integrated monitoring, logging, and trace managed services for applications and systems running on Google Cloud and beyond. For Google Workspace, 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. Google Cloud Access Transparency and Google Workspace Access Transparency are 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).	Ongoing Performance Monitoring
1.(4),2)	Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Regulated entities have the right to issue instructions to Google. Google will comply with the regulated entity's instructions. To issue instructions to Google, regulated entities can use the following functionality of the Services: Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. Google APIs: Application programming interfaces which provide access to Google Cloud.	Access; Rectification; Restricted Processing; Portability (Cloud Data Processing Addendum) Deletion by Customer (Cloud Data Processing Addendum) Compliance with Customer's Instructions (Cloud Data Processing Addendum)

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.(4),3)	Refer to your Google Cloud Financial Services Contract.	Governing Law
1.(4),4)	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Google Cloud infrastructure reliability guide whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications. For business continuity / disaster recovery scenario testing, in addition to testing our own environments, Google also provides a number of tools and resources that enable regulated entities to independently test their Google Cloud deployments. Our Disaster recovery scenarios for data and Disaster recovery scenarios for applications articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively. Google provides documentation for Google Cloud and Workspace to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	Technical Support
1.(4),5)	Google recognizes that regulated entities are expected to set impact tolerances on the assumption that a disruption will occur. Google is committed to enabling regulated entities to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article. We recognize that to remain within impact tolerances regulated entities often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud.	Business Continuity and Disaster Recovery
1.(4),6)	Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
1.(4),7)	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. To assist customers with their own incident response, Google's notification will describe: - the nature of the Data Incident including the Customer resources impacted; - the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; - the measures, if any, Google recommends that Customer take to address the Data Incident; and - details of a contact point where more information can be obtained. 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. - Agentic SOC orchestrates a dynamic system of AI agents that work together in a continuous loop to adapt to a changing security environment in real time, including autonomous triage and investigation, proactive threat hunting, and dynamic detection engineering. - Information on Google's security products is available here.	Data Incidents (Cloud Data Processing Addendum)

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities and threats; and helping you mitigate and remediate risks. - For Google Workspace, Security center provides advanced security information and analytics, and added visibility and control into security issues affecting your domain. The security center expands on advanced settings in the Google Admin console to surface your security data. 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. - Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. - Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. - Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Safeguarding access to your data" section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: - Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). - Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - 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).	Data Security; Additional Security Controls (Cloud Data Processing Addendum) Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
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. Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
1. (5)	Google will comply with all laws and regulations applicable to it in the provision of the Services.	Representations and Warranties

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	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. Investor Updates - Alphabet Investor Relations https://abc.xyz/investor/	Exclusion of Anti-Social Forces
1. (6)	**Termination:** Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or directed by the regulator. 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. **Data Deletion:** On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud whitepaper. **Transition assistance:** 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. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. 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. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here. For Google Workspace, detailed information is available on our Google Account help page. In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services. Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information. Google Cloud is committed to addressing customers' needs for portability and interoperability, and promoting openness to drive innovation. We provide organizations with tools to view, delete, download, and transfer their content. Cloud customers fully control their data and have the ability to take it out of Google Workspace and Google Cloud should they decide to switch to other platforms and/or store and process it on their own premises. **Advance notice due to termination of service deprecation:** Regulated corporations can decide on the advance notice period associated with the termination of service deprecation by entering into a direct contract with Google.	Term and Termination Deletion on Termination (Cloud Data Processing Addendum) Transition
1. (7)	Refer to your Google Cloud Financial Services Contract.	Liability
1. (8)	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination. 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.	Intellectual Property Protection of Customer Data

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
1. (9)	-	-
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. Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.	Protection of Customer Data Confidentiality
1. (9), 2)	For more information on Google's reporting, communication and incident response refer to 1. (4).	-
1. (10)	-	-
1. (10)	-	-
1. (11)	-	-
1. (11), 1)	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. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: provide information about our subcontractors; provide advance notice of changes to our subcontractors; and give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google 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. 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.	Google Subcontractors
1. (11), 2)	Google will remain accountable to you for the performance of all subcontracted obligations. Google will remain liable to you for any subcontracted obligations.	Google Subcontractors
1. (11), 3)	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 Subcontractors
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
1. (12)	Google grants audit, access and information rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity. 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. Google is committed to taking appropriate corrective or remedial actions if an audit on behalf of the regulated entity or the supervisory authority identifies unaddressed deviations in the Services operations and controls. Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy)	Enabling Customer Compliance Certifications and Audit Reports

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	-PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
1. (13)	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. This includes access to Google's premises used to provide the Services to conduct an on-site audit. 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. To assist customers with their own incident response, Google's notification will describe: - the nature of the Data Incident including the Customer resources impacted; - the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; - the measures, if any, Google recommends that Customer take to address the Data Incident; and - details of a contact point where more information can be obtained. 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. - Agentic SOC orchestrates a dynamic system of AI agents that work together in a continuous loop to adapt to a changing security environment in real time, including autonomous triage and investigation, proactive threat hunting, and dynamic detection engineering. - Information on Google's security products is available here. Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities and threats; and helping you mitigate and remediate risks. - For Google Workspace, Security center provides advanced security information and analytics, and added visibility and control into security issues affecting your domain. The security center expands on advanced settings in the Google Admin console to surface your security data. 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. - Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. - Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. - Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Safeguarding access to your data" section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools:	Enabling Customer Compliance Data Incidents (Cloud Data Processing Addendum) Data Security; Additional Security Controls (Cloud Data Processing Addendum) Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	- Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). - Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - 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).	
1. (14)	For details about deletion, including secure decommissioning when physical storage media reaches the end of its life-cycle refer to our Deletion on Google Cloud whitepaper. Deletion on Google Cloud https://cloud.google.com/docs/security/deletion Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Decommissioned Disks and Disk Erase Policy (Cloud Data Processing Addendum) Certifications and Audit Reports
1. (15)	Our support services are available in Japanese language. For more information about our language support refer to our Language Support page. Language support and working hours https://cloud.google.com/support/docs/language-working-hours	Technical Support
1. (16)	For more information on Google's reporting, communication and data incident response refer to 1.(4). For more information about traceability refer to 1.(4),7).	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
1. (17)	Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information. Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum) Data Incidents (Cloud Data Processing Addendum)
2.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page and Google Workspace Service Level Agreements page. The Technical Support Services Guidelines describe our support response times. Google Cloud Platform Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreements https://workspace.google.com/terms/sla.html Google Cloud Services Technical Support Services Guidelines https://cloud.google.com/terms/tssg Google Workspace Technical Support Services Guidelines https://workspace.google.com/terms/tssg/	Services Technical Support
3.	To assist you, Google provides the following reference information to help you considering countermeasures. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: - The Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. - Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. - Google Cloud's Observability is an integrated monitoring, logging, and trace managed services for applications and systems running on Google Cloud and beyond.	Ongoing Performance Monitoring

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Google Cloud infrastructure reliability guide whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications.	
4. (2)	Please refer to 1.(6) on data export and transition assistance. The cost of migration is transparent and based on our publicly listed service fees. Additionally, Google Cloud customers who wish to stop using Google Cloud and migrate their data to another cloud provider and/or on premises, can take advantage of free network data transfer to migrate their data out of Google Cloud. For more information, please refer to our blog post. 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
C22	Google is certified to the ISO27001 Standard, which regulates "Information security awareness, education and training" (ISO27001:2022, Annex A 6.3). Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Refer to our security whitepaper for more information.	-
C23	Google is certified to the ISO27001 Standard, which regulates controls for supplier relationships (ISO27001:2022, Annex A 5.19 to 5.22). Our information security administrative systems and vendor security initiatives, etc., are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google provides the following published information to help companies evaluate Google Cloud as an external provider. • The Google Security Whitepaper provides a comprehensive description of the various services available, as well as our systems for ensuring data security (protection of confidentiality) and integrity https://cloud.google.com/security/overview/whitepaper • Google can provide SOC audit reports through independent external auditors • On request, Google offers functionality for retrieving logs of instances in which Google Cloud accesses customer data. https://cloud.google.com/access-transparency • Customers can also refer to the following resources about our subprocessors: https://cloud.google.com/terms/subprocessors https://cloud.google.com/terms/data-processing-addendum (section 11. Subprocessors)	-
C24	When evaluating Google as an external provider, security measures can be taken through the following information and agreements.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	• The Google Security Whitepaper allows you to comprehensively check the availability of various services, as well as our systems for ensuring data security (protection of confidentiality) and integrity: Google Cloud Security Whitepaper https://cloud.google.com/security/overview/whitepaper Google Workspace Security Whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ • Google can provide SOC audit and similar reports through independent auditors. • Customers have the right to control their own data, including personal data. Google provides security services to help protect customer data. • For information on compliance with regulations, check the official page below: Compliance resource center https://cloud.google.com/security/compliance To review our data processing terms and data incident response process, please refer to the following resources: Cloud Data Processing Addendum https://cloud.google.com/terms/data-processing-addendum Data Incident Response Whitepaper https://cloud.google.com/docs/security/incident-response	
C25	-	-
C26	-	-
C27	-	-
C28	At Google Cloud, we believe that trust is created through transparency, and we work closely with our customers to help them meet due diligence, risk management, and regulatory compliance requirements. Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, Google provides resources to help customers evaluate the suitability of Google Cloud and Google Workspace as external providers. Please refer to what we documented in the Google Commentary for Control no.C20 for details. Google Cloud is dedicated to maintaining a robust Third Party Risk Management program that not only safeguards Google Cloud's operations but upholds the trust of Google Cloud's customers and partners. Google Cloud may engage third parties (Subcontractors) to perform specific activities in connection with the Google Cloud services. These Subcontractors are monitored and managed through Google Cloud's Third Party Risk Management (TPRM) program, which is designed to ensure that engagements with any Subcontractor uphold Google Cloud's high standards of security, compliance, and operational efficiency. For details, please refer to our Cloud Third Party Risk Management Resource Center.	-
P1	-	-
P2	-	-
P3	-	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
P4	Google Cloud and customers share responsibility for post-quantum cryptography (PQC) adoption, following a shared responsibility / shared fate model. Google is focused on securing its infrastructure, while customers are responsible for securing the upper layers. Recognizing the need for cloud-native PQC solutions, Google Cloud product teams are integrating PQC into relevant products to secure data, authentication, and key exchange. For the infrastructure and managed services that Google manages, no hardware replacement or system architecture changes will be required from customers. For customers who manage their own keys and cryptographic configurations, Google Cloud is developing guidance and tooling to ease their transition (“shared fate”). Learn more about how we are helping customers in Cloud with PQC: How we're helping customers prepare for a quantum-safe future Google Cloud assists with the Customer's PQC transition by: Regularly publishing updates on its PQC adoption journey as an example for other organizations (PQC Knowledge Hub). Offering expert advice through its Office of the CISO team to organizations beginning their PQC transformation (Office of the CISO). Providing consulting services, including Mandiant and Google Cloud Consulting, to help with security transformations and address questions on the correct cryptographic usage for PQC preparation.	-
P5	-	-
P6	-	-
P7	-	-
P8	-	-
P9	-	-
P10	-	-
P11	-	-
P12	-	-
P13	-	-
P14	Google is certified to the ISO27001 Standard, which regulates controls for information security incident (ISO27002:2022, Annex A 5.24 to 5.28), "Monitoring activities" (ISO27001:2022, Annex A 8.16), "Networks security" (ISO27001:2022, Annex A 8.20), "Security of network services" (ISO27001:2022, Annex A 8.21). Google uses sophisticated data processing pipelines to integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible incidents. Our investigation and incident-response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. We conduct Red Team exercises to measure and improve the effectiveness of our detection and response mechanisms. We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately. To review our data processing terms and data incident response process, please refer to the following resources: Cloud Data Processing Addendum https://cloud.google.com/terms/data-processing-addendum	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Data Incident Response Whitepaper https://cloud.google.com/security/incident-response You can refer to the following resource to review how security is designed into Google's technical infrastructure. https://cloud.google.com/docs/security/infrastructure/design	
P14-1	Google's security monitoring program is focused on information that's gathered from internal network traffic, from employee actions on systems, and from outside knowledge of vulnerabilities. A core Google principle is to aggregate and store all security telemetry data in one location for unified security analysis. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. We use a combination of open source and commercial tools to capture and parse traffic so that we can perform this analysis. A proprietary correlation system built on top of our technology also supports this analysis. We supplement network analysis by examining system logs to identify unusual behavior, such as attempts to access customer data. Our security engineers review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis and automated analysis of system logs helps determine when an unknown threat might exist; if the automated processes detect an issue, they escalate it to our security staff. For information about how you can monitor your workloads in Google Cloud, see Cloud Monitoring Security Command Center Monitoring integrity on Shielded VMs Refer to our security whitepaper for more information. Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. - Agentic SOC orchestrates a dynamic system of AI agents that work together in a continuous loop to adapt to a changing security environment in real time, including autonomous triage and investigation, proactive threat hunting, and dynamic detection engineering. - Information on Google's security products is available here. Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities and threats; and helping you mitigate and remediate risks. - For Google Workspace, Security center provides advanced security information and analytics, and added visibility and control into security issues affecting your domain. The security center expands on advanced settings in the Google Admin console to surface your security data.	-
P14-2	Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information. You can perform penetration testing of the Services at any time without Google's prior approval. In addition, Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	
P15	Google Cloud offers limited access points that can be accessed from external networks. Unnecessary communication ports and communication functions are blocked or restricted.	-
P16	Google is certified to the ISO27001 Standard, which regulates controls for information security incident (ISO27002:2022, Annex A 5.24 to 5.28), "Monitoring activities" (ISO27001:2022, Annex A 8.16), "Networks security" (ISO27001:2022, Annex A 8.20), "Security of network services" (ISO27001:2022, Annex A 8.21). Google uses sophisticated data processing pipelines to integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible incidents. Our investigation and incident-response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. We conduct Red Team exercises to measure and improve the effectiveness of our detection and response mechanisms. We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately. To review our data processing terms and data incident response process, please refer to the following resources: Cloud Data Processing Addendum https://cloud.google.com/terms/data-processing-addendum Data Incident Response Whitepaper https://cloud.google.com/security/incident-response You can refer to the following resource to review how security is designed into Google's technical infrastructure. https://cloud.google.com/docs/security/infrastructure/design	-
P17	-	-
P18	-	-
P19	Google is certified to the ISO27001 Standard, which regulates controls for information security incident (ISO27002:2022, Annex A 5.24 to 5.28), "Monitoring activities" (ISO27001:2022, Annex A 8.16), "Networks security" (ISO27001:2022, Annex A 8.20), "Security of network services" (ISO27001:2022, Annex A 8.21). Google uses sophisticated data processing pipelines to integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	incidents. Our investigation and incident-response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. We conduct Red Team exercises to measure and improve the effectiveness of our detection and response mechanisms. We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately. To review our data processing terms and data incident response process, please refer to the following resources: Cloud Data Processing Addendum https://cloud.google.com/terms/data-processing-addendum Data Incident Response Whitepaper https://cloud.google.com/security/incident-response You can refer to the following resource to review how security is designed into Google's technical infrastructure. https://cloud.google.com/docs/security/infrastructure/design	
P20	Google maintains malware protections for our core products (like Gmail, Google Drive, Google Chrome, YouTube, Google Ads, and Google Search) that use a variety of malware detection techniques. To discover malware files proactively, we use web crawling, file detonation, custom static detection, dynamic detection, and machine-learning detection. We also use multiple antivirus engines. To help protect our employees, we use the built-in advanced security capabilities of Chrome Enterprise Premium and the Enhanced Safe Browsing feature in Google Chrome. These capabilities enable proactive detection of phishing and malware sites as our employees browse the web. We also enable the most rigorous security settings that are available in Google Workspace, such as Gmail Security Sandbox, to proactively scan suspicious attachments. Logs from these capabilities feed into our security monitoring systems. In your Google Cloud environment, you can use Google Security Operations (SecOps), Security Command Center, and VirusTotal to monitor and respond to many types of malware. - Google Security Operations (SecOps)' cloud-native security operations platform empowers security teams to better detect, investigate, and respond to cybersecurity threats. - Security Command Center is a cloud-based risk management solution that helps security professionals to prevent, detect, and respond to security issues. - VirusTotal is an online service that analyzes files and URLs to identify viruses, worms, trojans, and other malicious content that's detected by antivirus engines and website scanners. Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information.	
P21	Google maintains malware protections for our core products (like Gmail, Google Drive, Google Chrome, YouTube, Google Ads, and Google Search) that use a variety of malware detection techniques. To discover malware files proactively, we use web crawling, file detonation, custom static detection, dynamic detection, and machine-learning detection. We also use multiple antivirus engines. To help protect our employees, we use the built-in advanced security capabilities of Chrome Enterprise Premium and the Enhanced Safe Browsing feature in Google Chrome. These capabilities enable proactive detection of phishing and malware sites as our employees browse the web. We also enable the most rigorous security settings that are available in Google Workspace, such as Gmail Security Sandbox, to proactively scan suspicious attachments. Logs from these capabilities feed into our security monitoring systems. In your Google Cloud environment, you can use Google Security Operations (SecOps), Security Command Center, and VirusTotal to monitor and respond to many types of malware. - Google Security Operations (SecOps)' cloud-native security operations platform empowers security teams to better detect, investigate, and respond to cybersecurity threats. - Security Command Center is a cloud-based risk management solution that helps security professionals to prevent, detect, and respond to security issues. - VirusTotal is an online service that analyzes files and URLs to identify viruses, worms, trojans, and other malicious content that's detected by antivirus engines and website scanners. Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information.	-
P22	Google maintains malware protections for our core products (like Gmail, Google Drive, Google Chrome, YouTube, Google Ads, and Google Search) that use a variety of malware detection techniques. To discover malware files proactively, we use web crawling, file detonation, custom static detection, dynamic detection, and machine-learning detection. We also use multiple antivirus engines. To help protect our employees, we use the built-in advanced security capabilities of Chrome Enterprise Premium and the Enhanced Safe Browsing feature in Google Chrome. These capabilities enable proactive detection of phishing and malware sites as our employees browse the web. We also enable the most rigorous security settings that are available in Google Workspace, such as Gmail Security Sandbox, to proactively scan suspicious attachments. Logs from these capabilities feed into our security monitoring systems. In your Google Cloud environment, you can use Google Security Operations (SecOps), Security Command Center, and VirusTotal to monitor and respond to many types of malware. - Google Security Operations (SecOps)' cloud-native security operations platform empowers security teams to better detect, investigate, and respond to cybersecurity threats. - Security Command Center is a cloud-based risk management solution that helps security professionals to prevent, detect, and respond to security issues. - VirusTotal is an online service that analyzes files and URLs to identify viruses, worms, trojans, and other malicious content that's detected by antivirus engines and website scanners.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information.	
P23	To assist you, Google provides documentation for Google Cloud and Workspace to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	-
P24	-	-
P25	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's infrastructure is designed to logically isolate each customer's data from the data of other customers and users, even when it's stored on the same physical server. Only a small group of employees have access to customer data. For Google employees, access rights and levels are based on an employee's job function and role, using the principles of least privilege and need-to-know that match access privileges to defined responsibilities. Google employees are granted only a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access must follow a formal process that involves a request and an approval from the data or system owner, manager, or other executives, as dictated by our security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to help ensure that approval policies are consistently applied. An employee's authorization settings are used to control access to resources, including data and systems for Google Cloud products. Support services are provided only to authorized customer administrators. Our dedicated security teams, privacy teams, and internal audit teams monitor and audit employee access, and we provide audit logs to you through Access Transparency for Google Cloud. Also, when you enable Access Approval, our support personnel and our engineers require your explicit approval to access your data. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation. To assist you, Google offers solutions for early detection of cloud misconfigurations and unauthorized security changes, including: - Security Command Center is a cloud-based risk management solution that helps security professionals to prevent, detect, and respond to security issues. Security Health Analytics is a managed service of Security Command Center that scans your cloud environments for common misconfigurations that might expose you to attack. - Risk and compliance as code (RCaC) codifies infrastructure and policies, and automate routine compliance checks.	-
P26	-	-
P27	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. 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. Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The “Safeguarding access to your data” section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google’s data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel’s location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - 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).	
P28	-	-
P29	-	-
P30	-	-
P31	Google provides documentation to explain how customers and their employees can use our services. If a customer would like more guided training, Google also provides a variety of courses and certifications.	-
P32	Refer to P20 and P21.	-
P33	-	-
P34	Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our Google Cloud security whitepaper and Google Workspace security whitepaper for more information. Google’s incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Google will notify you of data incidents promptly and without undue delay.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	More information on Google's data incident response process is available in our Data incident response whitepaper.	
P35	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. 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. Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Safeguarding access to your data" section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - 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).	-
P36	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. 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. Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	The “Safeguarding access to your data” section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google’s data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel’s location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - 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).	
P37	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. 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. Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The “Safeguarding access to your data” section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google’s data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel’s location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - The Status Dashboard provides status information on the Services.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	- Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. - 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).	
P38	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. 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. Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. The "Safeguarding access to your data" section of our Trusting your data with Google Cloud whitepaper and Trusting your data with Google Workspace whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. For Google Workspace; - 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).	-
P39	For Google Cloud, you can use Google Cloud Back Up and Disaster Recovery to manage backups. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. For Google Workspace, you can export their entire organization's data using Data Export. Google also has many tools that you can use to work with and extract your organization's Google Workspace data, such as APIs and BigQuery or partner solutions, such as Afi and SpinOne. For additional third-party and partner options, you can also check out our Google Cloud directory.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
P40	-	-
P41	-	-
P42	Google is certified to the ISO27001 Standard, which regulates controls for logical access (ISO27001:2022, Annex A 5.15 to 5.18, 8.2 to 8.5) and "Networks security" (ISO27001:2022, Annex A 8.20). Controls relating to Network Architecture and Management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's internal data access processes and policies are designed to prevent unauthorized persons and systems from gaining access to systems used to process Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Google's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)
P43	-	-
P44	-	-
P45	-	-
P46	-	-
P47	-	-
P48	Google is certified to the ISO27001 Standard, which regulates "Inventory of information and other associated assets" (ISO27001:2022, Annex A 5.9), "Acceptable use of information and other associated assets" (ISO27001:2022, Annex A 5.10), "Return of assets" (ISO27001:2022, Annex A 5.11), "Security of assets off-premises" (ISO27001:2022, Annex A 7.9), "Storage media" (ISO27001:2022, Annex A 7.10), "Equipment maintenance" (ISO27001:2022, Annex A 7.13), "Secure disposal or re-use of equipment" (ISO27001:2022, Annex A 7.14), and "Installation of software on operational systems" (ISO27001:2022, Annex A 8.19). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	-
P49	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
P50	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P51	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs,	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
P52	Google is certified to the ISO27001 Standard, which regulates "Equipment maintenance" (ISO27001:2022, Annex A 7.13).	-
P53	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
P54	Google is certified to the ISO27001 Standard, which regulates "Equipment maintenance" (ISO27001:2022, Annex A 7.13). Controls relating to management of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	-
P55	Google is certified to the ISO27001 Standard, which regulates "Capacity Management" (ISO 27001:2022, Annex A 8.6). Google has a robust network that monitors and adjusts capacity on an as-needed basis worldwide.	-
P56	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P57	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
P58	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P59	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
P60	Google is certified to the ISO27001 Standard, which regulates controls for physical and environmental Security (ISO27001:2022, Annex A 7.1 to 7.14). Google's focus on security and protection of data is among our primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, we use security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol our data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Very few Google employees will ever gain access to one of our data centers. Inside our data centers, we employ security controls in the physical-to-logical space, defined as "arm's length from a machine in a rack to the machine's runtime environment." These controls include hardware hardening, task-based access control, anomalous event detection, and system self-defense. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Security whitepaper : How Google protects the physical-to-logical space in a data center https://cloud.google.com/docs/security/physical-to-logical-space Google Workspace Security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P61	-	-
P62	-	-
P63	-	-
P64	-	-
P65	-	-
P66	-	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
P67	-	-
P68	-	-
P69	You can refer to the following docs to review service for protection of customer data. Sensitive Data Protection https://cloud.google.com/dlp/docs	-
P70	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. When an incident is detected, the Google Cloud Service Health team promptly notifies you, and provides regular updates while the incident is ongoing. All incidents undergo an internal retrospective to fully understand the incident and identify reliability improvements that Google can make. These improvements are then tracked and implemented. When incidents have very wide and serious impact, Google provides incident reports that outline the symptoms, impact, root cause, remediation, and future prevention of incidents. As with retrospectives, we pay particular attention to the steps that we take to learn from the issue and improve reliability. Google's goal in writing and releasing retrospectives is to be transparent and demonstrate our commitment to building stable products for our customers. For more information about incident communication and response, see the following white paper: Google Cloud Incident Communication https://docs.cloud.google.com/service-health/docs/incident-communication Incident Lifecycle	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
P71	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. When an incident is detected, the Google Cloud Service Health team promptly notifies you, and provides regular updates while the incident is ongoing. All incidents undergo an internal retrospective to fully understand the incident and identify reliability improvements that Google can make. These improvements are then tracked and implemented. When incidents have very wide and serious impact, Google provides incident reports that outline the symptoms, impact, root cause, remediation, and future prevention of incidents. As with retrospectives, we pay particular attention to the steps that we take to learn from the issue and improve reliability. Google's goal in writing and releasing retrospectives is to be transparent and demonstrate our commitment to building stable products for our customers. For more information about incident communication and response, see the following white paper: Google Cloud Incident Communication https://docs.cloud.google.com/service-health/docs/incident-communication Incident Lifecycle https://docs.cloud.google.com/service-health/docs/incident-lifecycle	-
P72	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. When an incident is detected, the Google Cloud Service Health team promptly notifies you, and provides regular updates while the incident is ongoing. All incidents undergo an internal retrospective to fully understand the incident and identify reliability improvements that Google can make. These improvements are then tracked and implemented. When incidents have very wide and serious impact, Google provides incident reports that outline the symptoms, impact, root cause, remediation, and future prevention of incidents. As with retrospectives, we pay particular attention to the steps that we take to learn from the issue and improve reliability. Google's goal in writing and releasing retrospectives is to be transparent and demonstrate our commitment to building stable products for our customers. For more information about incident communication and response, see the following white paper: Google Cloud Incident Communication https://docs.cloud.google.com/service-health/docs/incident-communication Incident Lifecycle https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
P73	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	
P73-1	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. 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.	-
P74	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-
P75	To assist you, Google provides a secure-by-design, secure-by-default infrastructure platform, as explained in the following whitepapers. Google security overview: https://cloud.google.com/docs/security/overview/whitepaper An Overview of Google's Commitment to Secure by Design: https://publicpolicy.google/resources/google_commitment_secure_by_design_overview.pdf	-
P76	-	-
P77	-	-
P78	-	-
P79	-	-
P80	-	-
P81	-	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
P82	Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud whitepaper.	-
P83	-	-
P84	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	- -
P85	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	- -
P86	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
P87	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-
P88	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
P89	To assist you, Google provides a secure-by-design infrastructure platform, as explained in the following whitepapers. Google security overview: https://cloud.google.com/docs/security/overview/whitepaper An Overview of Google's Commitment to Secure by Design: https://publicpolicy.google/resources/google_commitment_secure_by_design_overview.pdf	-
P90	-	-
P91	-	-
P92	-	-
P93	-	-
P94	-	-
P95	-	-
P96	-	-
P97	-	-
P98	-	-
P99	-	-
P100	-	-
P101	-	-
P102	Google is certified to the ISO27001 Standard, which regulates "Logging" (ISO27001:2022, Annex A 8.15) and "Monitoring activities" (ISO27001:2022, Annex A 8.16). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google Cloud uses internal and synthetic monitoring to detect incidents. For more information, see Chapter 6 of the Site Reliability Engineering book. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: The Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud's Observability is an integrated monitoring, logging, and trace managed services for applications and systems running on Google Cloud and beyond.	-
P103	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Google Cloud Service Health Dashboard and Google Workspace Status Dashboard provides status information on the Services. When an incident is detected, the Google Cloud Service Health team promptly notifies you, and provides regular updates while the incident is ongoing. All incidents undergo an internal retrospective to fully understand the incident and identify reliability improvements that Google can make. These improvements are then tracked and implemented. When incidents have very wide and serious impact, Google provides incident reports that outline the symptoms, impact, root cause, remediation, and future prevention of incidents. As with retrospectives, we pay particular attention to the steps that we take to learn from the issue and improve reliability. Google's goal in writing and releasing retrospectives is to be transparent and demonstrate our commitment to building stable products for our customers. For more information about incident communication and response, see the following white paper: Google Cloud Incident Communication https://docs.cloud.google.com/service-health/docs/incident-communication Incident Lifecycle https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
P103-1	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
P104	Google is certified to the ISO27001 Standard, which regulates "Information backup" (ISO27001:2022, Annex A 8.13) and "Redundancy of information processing facilities" (ISO27001:2022 Annex A 8.14). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps you protect your business from data loss. You can create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems. Google's systems are designed to minimize downtime or maintenance windows for when Google needs to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from design through operations, see the Google Cloud infrastructure reliability guide. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-
P105	-	-
P106	-	-
P107	-	-
P108	-	-
P109	-	-
P110	-	-
P111	-	-
P112	-	-
P113	-	-
P114	-	-
P115	-	-
P116	-	-
P117	-	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
P118	-	-
P119	-	-
P120	-	-
P121	-	-
P122	-	-
P123	-	-
P124	-	-
P125	-	-
P126	-	-
P132	-	-
P133	-	-
P134	-	-
P135	-	-
P136	-	-
P137	-	-
P138	-	-
P139	-	-
P140	-	-
P141	-	-
P142	-	-
P143	-	-
P144	-	-
P145	-	-
P146	-	-
P147	-	-
P148	-	-
P149	-	-
P150	Google's approach to developing and utilizing AI is anchored in its founding mission and guided by its long-standing AI Principles (published annually since 2019), which define explicit use-case boundaries and prioritize safety, fairness, privacy, and accountability. To demonstrate rigorous compliance, Google Cloud Platform, Google Workspace, and Gemini are certified under ISO/IEC 42001:2023, the international standard for Artificial Intelligence Management Systems (AIMS). Google’s AI readiness and processes have been independently validated by Coalfire against the NIST AI Risk Management Framework (AI RMF) and ISO/IEC 42001, confirming a "Mature" posture ready for enterprise risk governance. Internally, Google enforces multi-layered oversight through specialized forums, including Google DeepMind's Model Launch Review, centralized expert risk reviews, and the AGI forum.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	For customers, Google Cloud provides the Secure AI Framework (SAIF), which adapt traditional security megatrends (defense-in-depth, secure-by-design) to AI workloads, offering interactive risk self-assessments and agent risk maps. Google also co-founded the Coalition for Secure AI (CoSAI) with industry peers to establish standardized security measures across the ecosystem. For more details, please refer to the following documents: AI Principles - Google AI: https://ai.google/principles/ Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf ISO/IEC 42001 - Compliance | Google Cloud: https://cloud.google.com/security/compliance/iso-42001 Coalfire evaluates Google Cloud AI: 'Mature,' ready for governance, compliance: https://cloud.google.com/blog/products/identity-security/coalfire-evaluates-google-cloud-ai-mature-ready-for-governance-compliance?e=48754805 Responsible AI Progress Report (Published in February 2026): https://ai.google/static/documents/ai-responsibility-update-2026.pdf SAIF Risk Self-Assessment: https://saif.google/risk-self-assessment	
P151	Google Cloud provides comprehensive capabilities and tools to ensure the factual accuracy, auditability, and operational transparency of AI systems: - Grounding for Factual Accuracy: Google Cloud offers advanced grounding capabilities, including Grounding with Google Search, Web Grounding for Enterprise, and Grounding with Google Maps, which cross-reference prompts with verified enterprise data or live web indexes to minimize hallucinations and enhance the reliability of model responses. - Vertex AI Governance & Monitoring: Google integrates native tools such as Vertex Explainable AI (interpreting predictions), Model Evaluation (for quantitative metrics like BLEU or fairness/bias metrics), Model Monitoring (to detect drift and performance deviations in production), and Model Registry. - Model Armor: A fully managed service that screens LLM prompts and responses in real-time, defending against prompt injections, jailbreaks, malicious URLs, sensitive data leakage, and offensive content. - Adversarial Testing: Google utilizes its dedicated AI Red Team ("ethical hackers") to perform extensive pre-launch and post-launch testing to stress-test systems and proactively mitigate vulnerabilities. - Watermarking & Transparency: Google proactively watermarks synthetic media generated by its AI tools and publishes model cards and technical reports detailing model development, capability limits, and safety testing protocols. For more details, please refer to the following documents: Service Specific Terms | Google Cloud: https://cloud.google.com/terms/service-terms Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf Generative AI Risk Management in Financial Institutions: https://services.google.com/fh/files/misc/wp_generative_ai_risk_management_in_fs.pdf Google Cloud Services Summary: https://cloud.google.com/terms/services Generative AI, Privacy, and Google Cloud: https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf	-
P152	Google Cloud strictly enforces enterprise-grade safety, security, and privacy commitments under a Shared Responsibility Model: - Data Privacy & Training Restrictions: Google guarantees that "Your data is your data" and "Your data does not train our models"—Google will never use customer prompts or generated outputs to train its foundational models without prior permission. For fine-tuning, training data remains in the customer's secure instance, and learned parameters (adapter weights) are stored in a logically isolated layer accessible solely by the customer. - Supply Chain Security: Google secures its first-party models using the SLSA (Supply-chain Levels for Software Artifacts) framework and Sigstore, cryptographically signing model provenance to prevent tampering with model weights.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	- Data Protection & Infrastructure: Data is encrypted by default both at rest (AES-256) and in transit, with options for Customer-Managed Encryption Keys (CMEK via Cloud KMS). Customers can use VPC Service Controls to secure backend AI infrastructure and Sensitive Data Protection (formerly DLP) to scan, mask, or tokenize PII before ingesting datasets. - Generative AI IP Indemnification: Under a "shared fate" approach, Google provides a two-pronged intellectual property indemnity covering both the training data utilized by Google and the generated output from foundational models, assuming legal responsibility for copyright challenges if used responsibly. For more details, please refer to the following documents: Best Practices for Security Deploying AI on Google Cloud: https://services.google.com/fh/files/misc/best-practices-for-securely-deploying-ai-on-google-cloud.pdf Service Specific Terms | Google Cloud: https://cloud.google.com/terms/service-terms Generative AI, Privacy, and Google Cloud: https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf	
P153	Google Cloud actively supports customer enablement, AI literacy, and ecosystem security through diverse programs: - Technical Training & Certifications: Google provides extensive training resources, documentation, and specific learning paths (such as the Machine Learning Engineer Path) to ensure customers' personnel understand AI technology, model limitations, and compliance responsibilities. - Responsible Generative AI Toolkit: Google provides open-source developers and users with toolkits and methodologies to build safety classifiers, set proper content moderations, and establish custom safety filter thresholds. - Fostering Transparency and Guidance via Whitepapers: Google Cloud actively publishes research-backed guidance, tailored risk management frameworks for financial services, and whitepapers detailing how existing Model Risk Management (MRM) frameworks apply to generative AI. - Ecosystem Contribution: Google promotes open-source security tools (such as GKE's k8s-aibom for automated AI Bill of Materials) and actively collaborates with global regulatory bodies and standards organizations (NIST, ISO) to foster interoperable, safe AI practices. For more details, please refer to the following documents: Compliance resource center | Google Cloud: https://cloud.google.com/compliance Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf 7 key questions CISOs need to answer to drive secure, effective AI: https://cloud.google.com/blog/transform/7-key-questions-cisos-need-to-answer-to-drive-secure-effective-AI Applying model risk management guidance to artificial intelligence/machine learning based risk models https://services.google.com/fh/files/misc/wp_applying_existing_ai_ml_model_risk_management_guidance.pdf Generative AI Risk Management in Financial Institutions: https://services.google.com/fh/files/misc/wp_generative_ai_risk_management_in_fs.pdf Google's Secure AI Framework: https://saif.google/	-
F1	Google locates its data centers in areas that are not prone to various disasters.	-
F2	At Google data centers, we regularly conduct environmental inspections and take appropriate disaster measures.	-
F3	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F4	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F5	Google data centers feature a multi-layered physical security model with safeguards such as alarms, vehicle access barriers, and perimeter fencing.	-
F6	There are no signs indicating location of Google data centers.	-
F7	Google's data centers have appropriate lightning protection systems in accordance with the Building Standards Act and other relevant laws.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
F8	Google data centers are separated into sections and include safeguards such as custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. Access is granted only to approved employees with specific roles to enter.	-
F9	Google data centers use underground cables and non-combustible materials to prevent severing and spread of fire.	-
F10	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F11	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F12	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F13	Google data centers are protected by robust perimeter walls, etc.	-
F14	Google's data centers take measures to prevent the spread of fire in accordance with national and regional fire and fire prevention standards.	-
F15	Google data centers are equipped with alarmed security systems.	-
F16	Google's data centers have one entrance and exit that is used at all times, and we have implemented security measures such as security guards, contactless card entry, and the installation of surveillance cameras.	-
F17	Google data centers are equipped with emergency exits and place high importance on employee safety. Appropriate signage has been installed and training is carried out to ensure all staff can safely evacuate in the event of an emergency.	-
F18	Google's data centers take appropriate flood countermeasures based on an assessment of the environmental risks in the area.	-
F19	Robust, lockable doors are used at the entrances to Google data centers.	-
F20	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F21	Google data centers are designed to prevent collapse or damage during earthquakes.	-
F22	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. JQA-compliant server spaces are located above base isolation layers.	-
F23	Access to secure areas (e.g. server spaces) is only possible via security corridors. These security corridors implement multi-factor access control using security badges and biometrics. Access is granted only to approved employees with specific roles to enter. Access to these areas is monitored and recorded, and access privileges are periodically reviewed.	-
F24	Google room names are not displayed outside spaces leased from colocation providers. Colocation providers maintain fire-prevention floor plans and store them in locations inaccessible to third parties.	-
F25	Google data center server spaces are spacious enough for the operation and maintenance of equipment, and have safe evacuation routes in place. There is enough space to open and close doors without moving equipment.	-
F26	Google data center server spaces are in separate, dedicated zones.	-
F27	Server space in Google's data centers is limited to one entrance that is used at all times, and if the entrance door is left open for an extended period of time, an alarm will be activated and the monitoring center will be notified. Additionally, we have a policy prohibiting tailgating, and entrances and exits are monitored 24 hours a day remotely.	-
F28	Robust, lockable doors are used at the entrances to Google data center server spaces.	-
F29	All server spaces in Google data centers are windowless.	-
F30	Google data center server spaces have two way emergency exit routes, and high importance is placed on employee safety; appropriate signage has been installed and training is carried out to ensure all staff can safely evacuate in an emergency.	-
F31	Google data center server spaces are in separate, fireproof blocks in compliance with the Building Standards Act.	-
F32	Google data center server spaces are equipped with water leakage sensors. If the sensors are triggered, alerts are activated in the affected zone and DC operations control room.	-
F33	Google data centers continuously engage in ESD programs featuring guidance on ESD prevention. (ESD: Electrostatic discharge)	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
F34	Google data center server space interiors are made with non-flammable, fireproof materials.	-
F35	Google meets building requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Interiors, etc. are designed to prevent collapse or damage during earthquakes.	-
F36	The free access floor for server space in Google's data centers meets the earthquake risk and earthquake resistance standards of each country and region.	-
F37	Google data center facilities are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Fire detectors and extinguishers are in place to prevent damage to hardware. If a heat, fire, or smoke detector is triggered, alarms are activated simultaneously in the affected zone and DC operations control room.	-
F38	If a heat, fire, or smoke detector in a Google data center is triggered, alerts are activated simultaneously in the affected zone and DC operations control room.	-
F39	Google data center facilities are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Fire detectors and extinguishers are in place to prevent damage to hardware. If a heat, fire, or smoke detector is triggered, alarms are activated simultaneously in the affected zone and DC operations control room.	-
F40	Fire spread prevention measures have been taken to prevent the spread of fire at the penetrations from other sections of the server space at Google's data center.	-
F41	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F42	Google data center server spaces are equipped with emergency and portable lighting.	-
F43	Google data center server spaces are free from water-related facilities.	-
F44	At Google's data centers, they have installed and implemented appropriate measures based on disaster predictions in each region. For example, as part of our response standards in the event of an earthquake, they have installed earthquake detectors to measure the seismic intensity inside the building.	-
F45	Access to Google data center secure areas (e.g. server spaces) is possible, multidimensional access control using security badges and biometric authentication is required. In addition, access is granted to approved employees with specific roles to enter, which is regularly reviewed. An alarm is activated and a response system is in place.	-
F46	Environmental health and safety controls are enforced across Google data centers, and facilities implement adequate environmental safeguards in place. Temperature and humidity measurement and alarm devices are installed in appropriate locations and constantly monitored.	-
F47	Google meets building and facility requirements for the regions in which its data centers are located. In accordance with management standards for environmental sanitation in buildings as prescribed in the Act on Maintenance of Sanitation in Buildings, appropriate precautions are taken with regard to operation and maintenance, patrols, etc. There are also no kitchen or restaurant facilities inside the buildings.	-
F48	Appliances and equipment in Google data center server spaces are made with non-flammable materials.	-
F49	Environmental health and safety controls are enforced across Google data centers, and facilities implement comprehensive environmental safeguards. In addition to training on applicable standards, we continuously engage in ESD programs involving ESD prevention at all of our data centers. (ESD: Electrostatic discharge).	-
F50	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Equipment is fitted with safeguards against earthquakes.	-
F51	Carts (i.e. hand trucks) are permitted in Google data center server spaces to transport items in and out. They are not left inside the server spaces. All carts are equipped with locking mechanisms.	-
F52	Google meets building and facility requirements for the regions in which its data centers are located, and designs and constructs the data centers in line with best practices to limit damage to the greatest possible extent in the event of natural disasters.	-
F53	Google data center power and air-conditioning equipment rooms are spacious enough to operate and maintain equipment, and have safe evacuation routes in place. There is enough space to open and close doors without moving equipment.	-
F54	Google data centers have dedicated rooms for power and air-conditioning equipment. Access to power and air-conditioning equipment rooms is only granted to personnel who require entry for essential work purposes.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
F55	Google power and air-conditioning equipment rooms are windowless and have robust, lockable doors specifically designed to stop the spread of fire. Power and air-conditioning equipment rooms have one entrance.	-
F56	Environmental health and safety controls are enforced across Google data centers, and facilities implement comprehensive environmental safeguards. Power and air-conditioning equipment rooms are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire.	-
F57	Environmental health and safety controls are enforced across Google data centers, and facilities implement comprehensive environmental safeguards. Power and air-conditioning equipment rooms are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Fire detectors and extinguishers are in place to prevent damage to hardware. If a heat, fire, or smoke detector in a Google data center is triggered, alerts are activated simultaneously in the affected zone and DC operations control room.	-
F58	Environmental health and safety controls are enforced across Google data centers, and facilities implement adequate environmental safeguards in place. Power and air-conditioning equipment rooms are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Google data center power and air-conditioning equipment rooms are equipped with gas-based fire-extinguishing equipment. Additionally, fire extinguishers are placed in appropriate locations based on the fire regulations of each region.	-
F59	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F61	Google data center power facilities are designed and built with fail-safes.	-
F62	Google data centers are in operation 24 hours a day, with redundant power supplies and environmental management ensuring uninterrupted service. All critical components are equipped with main and alternative power sources supplying the same amount of power.	-
F63	Google data centers use uninterruptible power supply (UPS) systems to ensure stable operation of computer systems. In addition, through the use of backup generators, there is power to maintain maximum performance even in the event of an emergency.	-
F64	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F65	Google data centers are equipped with lightning arresters to prevent surges from grounding electrodes, and surge protection devices (SPDs) to discharge induced surges.	-
F66	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Equipment is fitted with safeguards against earthquakes.	-
F67	Google server spaces use dedicated circuits. Multiple power systems supply server spaces, and the power is routed through the facility appropriately.	-
F68	In Google server spaces, devices that may cause significant load fluctuations do not share the same power source.	-
F69	Google data centers use dedicated grounding for computer systems.	-
F70	In Google data centers, power supplies are wired from breakers and current leakage alarms are installed to protect each device from overcurrent.	-
F71	Google data centers use UPS power systems as a safeguard against disasters and criminal activity. In addition, through the use of backup generators, there is power to maintain maximum performance even in the event of an emergency.	-
F72	Google data center air-conditioning units are designed and built with fail-safes. The operating temperature of servers and other hardware is maintained at a fixed level, reducing the risk of service interruptions.	-
F73	Google installs and maintains cooling systems in accordance with industry best practices. Automatic controllers and anomaly alarms are installed, and the humidity and temperature of computer rooms are monitored, managed and appropriately adjusted.	-
F74	Google data centers use dedicated air-conditioning units for computer rooms.	-
F75	Google data centers are in operation 24 hours a day, with fail-safe redundancy systems, automatic controllers, and anomaly alarms ensuring uninterrupted service. Google installs and maintains cooling systems in accordance with industry best practices.	-
F76	Google data centers are in operation 24 hours a day, with fail-safe redundancy systems, automatic controllers, and anomaly alarms ensuring uninterrupted service. Google installs and maintains cooling systems in accordance with industry best practices.	-
F77	Google data centers have dedicated rooms for power and air-conditioning equipment. Access to power and air-conditioning equipment rooms is granted only to personnel who require entry for essential work purposes.	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
F78	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Equipment is fitted with safeguards against earthquakes.	-
F79	Google data centers use non-combustible materials for thermal insulation systems and air-conditioning unit vents to prevent damage in the event of a fire.	-
F80	Google data centers are equipped with central monitoring systems and surveillance equipment, etc. In the event of a failure or abnormality, the system immediately issues an alarm and responds accordingly.	-
F81	Google data centers are equipped with central monitoring systems and surveillance equipment, etc. In the event of a failure or abnormality, the system immediately issues an alarm and responds accordingly.	-
F82	In Google's data centers, circuit-related facilities are securely locked, and access is granted to personnel who require entry for essential work purposes. The doors to circuit-related facilities do not indicate the nature of the room.	-
F83	In Google's data centers, circuit-related facilities are securely locked, and access is granted to personnel who require entry for essential work purposes. The doors to circuit-related facilities do not indicate the nature of the room.	-
F83-1	In Google's data centers, lines are routed through dedicated circuits to prevent failures and unauthorized access.	-
F84	-	-
F85	-	-
F86	-	-
F87	-	-
F88	-	-
F89	-	-
F90	-	-
F91	-	-
F92	-	-
F93	-	-
F95	-	-
F96	-	-
F97	-	-
F98	-	-
F99	-	-
F100	-	-
F101	-	-
F102	-	-
F103	-	-
F104	-	-
F105	-	-
F106	-	-
F107	-	-
F108	-	-

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
F109	-	-
F110	-	-
F111	-	-
F112	-	-
F113	-	-
F114	-	-
F115	-	-
F116	-	-
F117	-	-
F118	-	-
F119	-	-
F120	-	-
F121	-	-
F122	-	-
F123	-	-
F124	-	-
F125	-	-
F126	-	-
F127	-	-
F128	-	-
F129	-	-
F130	-	-
F131	-	-
F132	-	-
F133	-	-
F134	-	-
F138	-	-
A1	Google grants audit, access and information rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity. 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. Google is committed to taking appropriate corrective or remedial actions if an audit on behalf of the regulated entity or the supervisory authority identifies unaddressed deviations in the Services operations and controls.	Enabling Customer Compliance Certifications and Audit Reports

#	Google Cloud commentary	Google Cloud Financial Services Contract reference
	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
A1-1	-	-