Google Cloud Whitepaper
August 2026

Google Cloud User Guide to QCB's Cloud Computing Regulation

Authors: Akshay Dalal, Joe Tan

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of August 2026 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Abstract

As Qatar's financial sector continues its rapid digital transformation, financial institutions must navigate a clear and robust regulatory framework established by the Qatar Central Bank (QCB). This guide is here to help you, as a QCB-licensed entity, confidently adopt and expand your use of Google Cloud in alignment with Qatar's dual framework covering both cloud outsourcing and data protection.

This guide highlights Google Cloud's core commitment to security and compliance and details how Google Cloud security and compliance capabilities can be mapped to the key domains addressed in the QCB Cloud Computing Regulation and the QCB Data Handling and Protection Regulation. This includes IT governance, risk management, due diligence, cyber defense, robust data handling, data residency, and business continuity. It further presents a detailed mapping of how Google Cloud can help you comply with specific requirements in the QCB's Cloud Computing framework. By using this guide, you can learn how to leverage Google Cloud's secure infrastructure and tools to meet your security and regulatory goals.

Ultimately, this resource empowers you to build a robust risk governance framework for effectively managing IT risks, strengthening cybersecurity, protecting sensitive data, and ensuring operational continuity, accelerating your secure adoption of Google Cloud.

Google Cloud's Commitment to Security and Compliance

At Google Cloud, security and compliance are integral to the design and operation of our platform. We understand that for financial institutions, trust is paramount, and independent verification of security, privacy, and compliance controls is essential. Our fundamental approach is to deliver a highly secure and resilient infrastructure, complemented by a comprehensive suite of tools and services that empower you to protect your data and applications effectively.

To offer this assurance, Google Cloud undergoes regular, independent third-party audits. We are committed to adhering to key international standards that provide a robust framework for meeting the requirements of the QCB on financial institutions. These include: 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, and ISO 42001 (Artificial Intelligence Management Systems). These certifications validate our rigorous controls over information security, cloud-specific security, privacy for personal data in the cloud, financial reporting controls, and AI management systems, establishing a credible basis for your own compliance initiatives. You can access Google's current certifications and audit reports at any time via our Compliance Reports Manager, which provides streamlined, on-demand access to these crucial compliance resources.

Key QCB Regulations to Consider for Cloud Adoption

For financial institutions in Qatar, adopting cloud services requires navigating a multi-layered regulatory landscape established by the Qatar Central Bank (QCB). It is essential to understand how these regulations

interlink to form a comprehensive governance and security framework. The following regulations and guidelines, published by the QCB, are key considerations for any cloud outsourcing arrangement.

Primary Regulations for Cloud and Data

These two regulations form the foundation for any cloud adoption journey by a QCB-licensed entity:

- **Cloud Computing Regulation:** This is the cornerstone regulation, providing a detailed framework for the entire cloud lifecycle. It governs the mandatory requirements for strategy, due diligence on service providers, risk assessment, contractual terms, ongoing monitoring, operational security, and exit planning.
- **Data Handling and Protection Regulation:** This regulation works in close concert with the Cloud Computing Regulation, focusing specifically on the governance of data itself. It mandates the creation of a data classification framework, sets strict data residency rules requiring the primary environment for sensitive data to be within Qatar, and outlines requirements for data retention and third-party access.

Sector-Specific Security Regulations

The QCB provides more granular security instructions tailored to different financial sub-sectors. Institutions must comply with the regulation applicable to their license. These include, but are not limited to:

- **Insurance Sector Cyber Security Regulation:** Provides specific cybersecurity requirements for insurance companies, including detailed controls for cloud computing (Section 8.9).
- **Information and Cyber Security Regulation for Payment Service Providers:** Outlines the security framework for PSPs, with a dedicated section on managing the risks of cloud computing (Section 6).
- **Technology Risk Instructions for Financial Services Operators:** Applies to entities like exchange houses and investment companies, and includes specific instructions for establishing a cloud computing policy, ensuring data residency, and managing cryptographic keys (Section 1.8).

Foundational Circulars and Guidelines

These documents address broader technology principles and emerging areas that are directly relevant to cloud usage:

- **Technology Risks Circular (January 2018):** A foundational circular that provides broad guidance on managing technology and e-banking risks. Its principles on risk management, business continuity, and outsourcing, are directly applicable to cloud arrangements.
- **Artificial Intelligence Guideline:** For institutions planning to leverage cloud-based AI and Machine Learning services, this guideline is essential. It explicitly references the Cloud Computing Regulation and sets requirements for AI governance, risk management, and outsourcing when using AI systems.

Underpinning consumer data protection

Finally, all activities must comply with Qatar's national privacy law:

- **Law No. (13) of 2016 on Personal Data Privacy Protection (PDPPL):** This is the foundational law governing the processing of all personal data in Qatar. As a Data Controller, your institution is ultimately responsible for ensuring that all data processing, whether on-premises or in the cloud, adheres to the principles and obligations of this law.

Please note: Regulations are changing rapidly in this space, and Google Cloud is working to help customers proactively respond to new rules and guidelines. Google Cloud encourages its customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including other local regulations, guidelines and laws.

Google Cloud provides the technical capabilities and a shared responsibility model that can help your organization meet these regulatory expectations. The following sections provide more information on how we can support your journey to regulatory compliance.

Enabling Your Compliance

The QCB regulations generally place significant emphasis on key aspects of IT governance and IT service provider management, risk management and compliance, cyber defense and security, data management and governance, and data residency and cross-border transfers. Google Cloud offers a comprehensive set of services and features that customers can leverage to address these core domains.

Addressing shared aspects of the regulations

IT Governance and IT Service Provider Management

The regulations underscore the importance of banks' effective IT governance and risk management when engaging with IT service providers. Google Cloud operates on a transparent model where customers retain control over their services. You determine which services to utilize, how to configure them, and their specific purpose, ensuring your organization maintains oversight of relevant activities.

- **Control and Management Tools:** You can manage your Google Cloud resources using the Cloud Console (a web-based graphical user interface), the gcloud Command Tool (our primary command-line interface for Google Cloud), and Google APIs (Application Programming Interfaces that provide programmatic access to Google Cloud). These interfaces enable granular control over your cloud environment.
- **Performance Monitoring and Transparency:** You can continuously monitor Google's performance of the services, including adherence to Service Level Agreements (SLAs). The Service Health Dashboard provides real-time status information on Google Cloud services. Personalized Service Health filters disruptive events relevant to your projects, helping you assess impact and maintain business continuity.
- **Google Cloud Operations** (which includes Cloud Logging, Cloud Monitoring, and Cloud Trace) offers an integrated solution for monitoring, logging, and diagnostics, providing deep insights into your applications running on Google Cloud, including service availability and uptime.
- **Access Transparency:** This Google Cloud feature provides logs of actions taken by Google personnel concerning your data. Log entries include the affected resource, the time of action, the reason for the action (e.g., the case number associated with a support request), and data about the Google personnel involved (e.g., their location). This offers visibility and auditability into Google's operations, directly supporting your oversight requirements for IT service providers. Additionally, Access Approval 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.

Risk Management and Compliance

The regulations also highlight the increased IT risk exposure for banks, including cyber incidents and data

leakage. Google Cloud understands your need to conduct due diligence and perform comprehensive risk assessments before adopting our services.

- **Due Diligence and Third-Party Risk Management (TPRM):** We provide extensive documentation and resources to support your due diligence processes. Google collaborates with independent TPRM providers who conduct regular assessments of Google Cloud's platform and services. These assessments examine 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, and SOC2. The resulting independent audit reports can help streamline and accelerate your internal risk assessment processes. For more information, refer to our Google Cloud Third Party Risk Management Resource Center.
- **Proven Experience and Corporate Information:** With over a decade of providing cloud services, Google Cloud supports customers across diverse sectors globally, including financial services. Our Financial Services Cloud Blog and Financial Services solutions page detail how financial institutions leverage Google Cloud to drive business transformation, foster data-driven innovation, and meet security and compliance objectives. Information about Google's corporate history, mission, business model, strategy, organizational policies (including our Code of Conduct) and audited financial statements are available on Alphabet's Investor Relations page. You can also review information about Google's historical service performance on our Google Cloud Service Health Dashboard.

Cyber Defense and Security

Another significant focus is on strengthening IT organization management to mitigate risks, particularly cyber incidents. Google Cloud provides robust cybersecurity capabilities integrated throughout our infrastructure and services.

- **Security of Google's Infrastructure:** Google manages the security of our infrastructure, encompassing the hardware, software, networking, and facilities that support the Services. We provide detailed information about our security practices, including our infrastructure security page, security whitepaper, infrastructure security design overview page, and security resources page. To help protect customer data, we run an industry-leading information security operation that combines stringent processes, an expert incident response team, and multi-layered information security and privacy infrastructure.
- **Security of Your Data and Applications:** You define the security measures for your data and applications within the cloud. Google proactively takes steps to assist you, including **encryption at rest** (enabled by default with no additional action required from you, as detailed on the Google Cloud Encryption at rest page) and **encryption in transit** (encrypting and authenticating all data when it moves outside physical boundaries not controlled by Google or on behalf of Google, as detailed on the Google Cloud Encryption in transit page). Our SOC 2 report attests to the design and operating effectiveness of controls related to the Trust Services Criteria of security, availability, processing integrity, confidentiality, and privacy. It specifically covers Google's controls that protect customer data within the Google Cloud Platform system, including logical and physical access, system operations, and change management.
- **Security Products and Resources:** You can enhance and monitor your data's security using a wide range of Google's security products and services:
    - Security Command Center (SCC) provides a centralized platform for managing security and risk across your cloud environment. It offers capabilities to prevent, detect, and respond to security issues by integrating services that address vulnerability detection, threat detection, compliance monitoring, and security posture management. SCC helps you gain comprehensive visibility into your assets, identify misconfigurations and threats, and offers tools for effective remediation to strengthen overall cloud security.

- Google Cloud Armor offers robust, global protection against DDoS attacks and provides Web Application Firewall (WAF) services with customizable rules, helping ensure the availability and security of your internet-facing applications.
- reCAPTCHA Enterprise protects websites and applications from fraudulent activity and spam by distinguishing between human users and bots.
- Google Threat Intelligence capabilities leverage Google's vast global network and security expertise to provide customers with continuously updated, actionable insights into emerging threats, enabling proactive defense against sophisticated attacks.
- Google Security Operations unifies security operations with AI-powered analytics to accelerate threat detection, investigation, and response, ultimately strengthening customer security posture.
- Mandiant Cybersecurity Consulting offers strategic services like cyber defense transformation and incident response, enabling customers to proactively enhance their defenses and effectively respond to evolving threats.

Data Management and Governance

The regulations stress the importance of preventing customer personal data leakage and ensuring appropriate data management practices. Google Cloud offers services that facilitate robust data governance, protection, and responsible data processing.

- **Data Access and Use Commitments:** Google commits to accessing or using your data solely to provide the Services you ordered and will not use it for any other Google products, services, or advertising.
- **Subcontractor Compliance:** We require our subcontractors to meet the same high standards, ensuring they comply with our contract with you and only access and use your data as required to perform their subcontracted obligations.
- **Data Protection Laws & Regulations:** Google complies with all national data protection regulations applicable to it in the provision of the Services, as addressed in the Cloud Data Processing Addendum. We are committed to upholding robust data privacy and security measures, including strong contractual commitments, encryption, and transparent practices.
- **Data Loss Prevention: Sensitive Data Protection** helps you discover, classify, and protect sensitive data across your Google Cloud environment, preventing unauthorized access and leakage. It can scan various data sources for sensitive information, such as national identification numbers, credit card numbers, and other personally identifiable information (PII).
- **Secure Data Storage and Analytics: Cloud Storage** provides highly durable, available, and secure object storage for all your data, with options for encryption at rest and in transit. **BigQuery**, our fully managed, petabyte-scale data warehouse, offers robust security features including column-level encryption, row-level security, and auditing capabilities, enabling secure data analytics while maintaining compliance. Services like **Dataproc** allow for secure and compliant processing of large datasets.

Data Residency

The Data Handling and Protection Regulation (Section 7.6) and Cloud Computing Regulation (Section 21.4) require that PII, SPI, and SFI must have their primary processing and storage environment within the State of Qatar.

- **Region Selection:** Google Cloud offers regions globally, including the **Doha (me-central1)** region in Qatar). The Doha region consists of three or more zones housed in three or more physical data centers. You maintain control over where your data at rest is stored by selecting this specific Google Cloud region for your resources. This capability allows you to deploy your systems and store your sensitive data

within Qatar, directly supporting data residency requirements.

- **Data Location and Encryption:** All data stored in Google Cloud is encrypted at rest and in transit. You retain control over your data's location, and our contractual terms specify our commitments regarding data residency and data handling. For particular services, you can configure data residency policies to ensure data remains within designated geographic boundaries, minimizing the need for cross-border transfers where prohibited. More information is available in our Google Cloud Trust Center.
- **Data Incident Response:** 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 process. To assist customers with their own incident response, Google's notification will describe the nature of the data incident, including impacted customer resources; measures Google has taken or plans to take; recommended customer actions; and details of a contact point for more information.
- **Controlled Approach to Government Data Requests:** Google has a rigorous and transparent process for handling government requests for cloud customer data, emphasizing a strong commitment to data protection by carefully evaluating each request, challenging overly broad demands, and providing robust security and privacy controls to customers.

Business Continuity and Exit Planning

The QCB requires robust, tested plans for business continuity and exit planning

- **Disaster Recovery (DR) and Resilience:** Google Cloud implements a business continuity plan for the Services, reviewed and tested at least annually. Our data centers are certified as ISO 22301 compliant.
- **Exit Planning and Data Portability**: Google is committed to data portability and open-source to help you address vendor lock-in and plan for exit. We will enable you to access and export your data throughout the duration of our contract and during a post-termination transition term. Upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract to support a smooth transition.

Qatar National Information Assurance (NIA)

- Qatar National Cyber Security Agency's (NCSA) approved National Information Assurance (NIA) policy is a comprehensive framework based on the best practices of leading organizations and international standards. It is designed to guide organizations in implementing effective information security controls. The NIA policy assists organizations in protecting their information assets, managing risks, complying with regulations, and achieving international standard certifications. NCSA requires a third-party assessment of any organization interested in being certified against the NIA policy. The robust certification process requires that a third party assess a cloud provider's security controls and compliance with Qatari laws and regulations.
- Google Cloud has obtained Qatar's NIA certification through an accredited third-party assessment organization that has attested that Google Cloud meets the highest Qatari security and compliance standards. The certification applies to the Belgium, Netherlands and Qatar regions.

Compliance with QCB's Cloud Computing Regulation in the context of Google Cloud

This table below is designed to help an organization supervised by the Qatar Central Bank ("regulated entity") to consider Cloud Computing Regulation ("framework") in the context of Google Cloud Platform ("GCP") and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: Part C (Cloud Computing Lifecycle) and Part D (Operational Security Controls). For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
PART C (CLOUD COMPUTING LIFECYCLE)		
10. Entity Outsourcing Implementation Planning		
10.1. An Entity must plan and manage its transition to a Cloud Service Provider (CSP). This should include an evaluation of the CSP's technical support capabilities and any guidance or tools they can provide to facilitate a smooth transition of functions.	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk. As part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards from around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit	N/A

	reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information.	
10.2. An Entity must review its governance and data requirements, and check for any constraints before planning a transition to the cloud, this includes but is not limited to:		

10.2.1. An Entity must conduct a legal due diligence to ensure that it is not restricted by legal obligations, QCB issued regulations, or agreements, or data use agreements that might restrict the transfer of data to third parties, even if these third parties are service providers.	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 will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. 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. 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	N/A Representations and Warranties Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)

	choose where to store your data, Google will not store it outside your chosen region(s).	
10.2.2. An Entity must check that the required consent has been received as per the Law No. (13) of 2016 on Personal Data Privacy Protection, if the company plans to subcontract the processing of the Customer's data to a third party.	Google will comply with our obligations under the GDPR regarding authorization for subprocessing.	Processing of Data; Subprocessors (Cloud Data Processing Addendum)
10.2.3. An Entity must review the legal and regulatory requirements, contractual obligations and other corporate policies. Corporate policies and standards must be reviewed to see if they need to be updated to allow a third party to handle data.	Refer to our commentary on Clause 10.2.1.	N/A
10.2.4. An Entity must ensure data governance policies and practices extend to data processed on the cloud.	Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image. Secure Service Deployment We use cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand. Refer to our infrastructure security page for more information.	Access and Site Controls (Cloud Data Processing Addendum)
10.2.5. An Entity must review whether the existing data or technical architectures are optimal for a cloud environment prior to migrating to the cloud.	Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page. In addition, Google Cloud's Architecture Framework provides recommendations and describes best practices to help you design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.	N/A

	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk.	
11. Cloud Computing Arrangement Due Diligence		
11.1. An Entity must undertake due diligence on the CSP whether it is directly contracted with the CSP or has contracted with a CSP via a broker or other intermediary.	Refer to our commentary on Clauses 10.2.1 and 10.2.5.	
11.2. An Entity must undertake due diligence on prospective CSP and appropriateness of the prospective CSP and services selected, considering the intended usage of the Cloud Computing service.	Refer to our commentary on Clauses 10.2.1 and 10.2.5.	
11.3. An Entity must have a clear and documented business case or rationale in support of the decision to utilize the cloud.	This is a customer consideration.	N/A
11.4. An Entity must consider the CSP's data confidentiality, security maturity, financial, operational, and reputational factors and the CSP's ability to comply with its obligation under the outsourcing arrangement, in its due diligence of a service provider.	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

	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: Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on	

	behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: Security best practices Security use cases Security blueprints Technical capacity / service delivery / reputation Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. You can review information about Google's historic performance of the services on our Google Cloud Service Health Dashboard.	N/A

	Corporate information Information about Google's corporate history is available on Alphabet's Investor Relations page. You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. You can review Google's audited financial statements on Alphabet's Investor Relations page. 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, which addresses conflicts of interest Compliance As part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards from around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information.	
11.5. An Entity must consider its data classification framework and the sensitivity of data in scope prior to any Cloud Computing Arrangement.	This is a customer consideration.	N/A
11.6. An Entity must ensure that the depth of the due diligence must commensurate with the criticality and Materiality of the Cloud Computing Arrangement.	This is a customer consideration.	N/A
11.7. An Entity must establish risk mitigating controls that align with the criticality and Materiality of the Cloud	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on	Data Export (Cloud Data Processing Addendum)

Computing Arrangement and deploy cloud model-specific (SaaS, PaaS, IaaS) controls.	customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud. In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page.	
11.8. An Entity must consider the track record of the CSP in achieving acceptable outcomes in areas such as information security policies and awareness, due diligence and risk assessment of practices related to sub-contracting, system vulnerability assessments, penetration testing and technology refresh management.	Information security policies and awareness 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)	Certifications and Audit Reports

	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. Subcontracting 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 the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable. System vulnerability assessments 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	Google Subcontractors Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

	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 security whitepaper for more information. Penetration testing Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Customer Penetration Testing
11.9. An Entity must verify the CSP's ability to recover the outsourced systems and/ or IT services within the stipulated Recovery Time Objective ("RTO") & Recovery Point Objective ("RPO").	Refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired RTO and RPO for your applications.	N/A
11.10. An Entity must cover all zones that support the Entity's processing and data storage requirements in its due diligence of a CSP. It must not be assumed that controls are consistent across all locations. An Entity must set the scope of the due diligence assessment appropriately to cover an adequate set of controls and individual assessments of all locations expected to be relevant in the arrangement.	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. 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.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

	-Google makes the same commitments about all its subprocessors, regardless of country / region.	
11.11. An Entity must ensure that CSP implement strong authentication, access controls, data encryption and other security and technical controls to meet the Entity's requirements.	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 “Managing Google’s Access to your Data” section of our Trusting your data with Google Cloud 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	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)

	Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	
11.12. An Entity must verify that the CSP's controls adhere to the QCB Sector-Specific Security Regulation.	The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment. In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Board of Directors Handbook for Cloud Risk Governance and Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud.	N/A
11.13. Prior to implementing Cloud Computing services and undertaking an outsourcing arrangement, an Entity must conduct an initial security and risk assessment of the service to identify any information security, cybersecurity other IT control weaknesses. This must be done as per the Entity's internal processes and the Sector-Specific Security Regulation.	Refer to our commentary on Clause 11.4.	
11.14. An Entity must ensure that the security and risk assessment identifies security threats including information security threats and operational weaknesses and develop safeguards to mitigate those threats and weaknesses. The factors considered during the risk assessment must include, but are not limited to the following:		
11.14.1.Nature of the service (including specific underlying arrangements).	The Google Cloud services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions

11.14.2. Provider and the location of the service.	Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page.	N/A
11.14.3. Criticality and confidentiality of the assets involved.	Refer to our commentary on Clause 11.4.	
11.14.4. Transition process including handover from an Entity and/ or other service providers to the potential outsourcing service provider.	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.	Transition Assistance
11.14.5. Adherence to recognized technical security standards.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ISO/IEC 27001 (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.	Certifications and Audit Reports
11.14.6. Compliance with international and domestic standards.	Refer to our commentary on Clause 11.14.5.	

11.14.7. An Entity may also take any external assurance that has already been provided by independent auditors when conducting their own due diligence.	Refer to our commentary on Clause 11.14.5.	Customer Information, Audit and Access
11.15. An Entity must conduct a Threat & Vulnerability Risk Assessment (TVRA) or an equivalent independent assessment on the CSP's data centers where these data centers support the Entity's operations.	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. These rights apply regardless of the service location.	Regulator Information, Audit and Access Customer Information, Audit and Access
11.16. An Entity must ensure the CSP has a disaster recovery and business continuity plan.	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
11.17. An Entity must conduct a detailed review of any financial information publicly available, provided by the CSP or other sources, in its due diligence.	Information about Google's corporate history is available on Alphabet's Investor Relations page. You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. You can review Google's audited financial statements on Alphabet's Investor Relations page. 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, which addresses conflicts of interest.	N/A

11.18. An Entity must assess its Cloud Computing Arrangements compliance to the global standards as per the clause (8.4) and this regulation. For such purposes, an Entity may rely on an independent reputable auditor's assurance demonstrating the CSP's compliance.	Refer to our commentary on Clauses 11.14.5 and 11.15.	
12. Sub-Contractors Due Diligence		
12.1. If the Entity, by the contract with the CSP, permits sub-contracting of material or important functions (or material parts thereof), the Cloud Computing Arrangement must:		
12.1.1 Specify any part or aspect of the outsourced function that are excluded from potential sub-contracting.	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. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would potentially be denying all our customers the benefit motivating the subcontracting arrangement. To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice.	Subcontracting; Google Subcontractors
12.1.2 Indicate the conditions to be complied with in case of sub-contracting.	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: -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 Subcontractors
12.1.3. Specify that the CSP remains accountable and is obliged to oversee those services that it has	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors	Google Subcontractors

sub-outsourced to ensure that all contractual obligations between the CSP and an Entity are continuously met.	comply with our contract with you (including the audit and access rights) and applicable law and regulation. Google will remain accountable to you for the performance of all subcontracted obligations.	
12.1.4. Include an obligation for the CSP to notify an Entity of any intended sub-contracting, or material changes thereof, in particular where that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the Entity. The notification period set in the written agreement must allow an Entity sufficient time at least to carry out a risk assessment of the proposed sub-contracting or material changes thereof and to object to or explicitly approve them.	You need enough time from being informed of a subcontractor change to perform a meaningful risk assessment before the change comes into effect. To ensure you have the time you need, Google provides advance notice before we engage a new subcontractor or change the function of an existing subcontractor.	Google Subcontractors
12.1.5. Ensure that an Entity has the right to object to the intended sub-contracting, or material changes thereof, or that explicit approval is required before the proposed sub-contracting or material changes come into effect.	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
12.1.6. Where an Entity does not have the contractual right to reject any proposed subcontractor, it is recommended that an Entity must retain a right to terminate the agreement.	Refer to our commentary on Clause 12.1.5.	
12.2. An Entity must review the sub-contracting arrangements relevant to the provision of a regulated activity to determine if these sub-contacting arrangements ensure its compliance with regulatory requirements.	Google recognizes that subcontracting must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
12.3. The Entity must ensure that any subcontractor processing an Entity's data must adhere to the same QCB requirements adhered to by the CSP.	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you and to only access and use your data to the extent required to perform the obligations subcontracted to them.	Google Subcontractors
13. Contractual Considerations		
13.1. An Entity must ensure that the respective rights and obligations of an Entity and its CSP are clearly set out in a written agreement, either directly or through an intermediary	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A

(who may also be providing elements of the Cloud Computing).		
13.2. An Entity must ensure that written agreement expressly allows the possibility for an Entity to terminate it, where necessary.	Regulated entities can elect to terminate our contract for convenience with advance notice, including: -if necessary to comply with law; and -if directed by a supervisory authority; and -if Google increases the fees.	Term and Termination
13.3. An Entity must ensure that its written agreement for a Material Arrangement addresses the following issues including, but not limited to:		
13.3.1. A clear description of the outsourced function.	The Google Cloud services are described on our services summary page.	Definitions
13.3.2. SLAs: Enforceable and measurable SLAs must include a definition of the governance to be put in place to manage the contract on an ongoing basis. This must define any management information and other deliverables that will form the basis for that governance.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
13.3.3.The start date and end date, where applicable, of the agreement and the notice periods for the CSP and for the Entity.	Refer to your Google Cloud Financial Services Contract.	Term and Termination
13.3.4.The roles, relationships, obligations and responsibilities of all contracting parties.	Refer to our commentary on Clause 13.1.	N/A
13.3.5. Ownership and control over IT Assets, if the CSP is expected to be given some level of control over IT Assets, this level of control must be defined in the relevant outsourcing agreement.	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.	Intellectual Property
13.3.6. Provisions regarding information security and protection of personal data and proof these satisfy the requirements of the Law No. (13) of 2016 on Personal Data Privacy Protection in addition to the Sector-Specific Security Regulation issued by QCB.	Google will comply with all national data protection regulations applicable to it in the provision of the Services. This is addressed in the Cloud Data Processing Addendum.	Representations and Warranties
13.3.7. The requirement for the CSP to grant the Entity, its competent authorities, and any other person appointed by an Entity or the competent authorities the right to access data and business premises and audit the same.	Refer to our commentary on Clause 11.15.	

13.3.8. An Entity must have the right to monitor, review and audit Cloud Computing Arrangements. This can be by the Entity's internal control functions, and regulators, or persons employed by them, including for the purposes of supervisory reviews by QCB.	Refer to our commentary on Clause 11.15.	
13.3.9. An Entity must ensure that it receives reports relevant to its security function and key functions from the CSP, such as reports prepared by the internal audit function of the CSP.	Refer to our commentary on Clause 11.14.5.	

13.3.10. An Entity must receive detailed data on cyber security arrangements from the CSP such as but not limited to: Malware protection, cryptographic controls, security testing, technical compliance, KPI (Key Performance Indicators) & KRI (Key Risk Indicators).	Google's malware prevention strategy begins by preventing infection using manual and automated scanners to scour our search index for websites that might be vehicles for malware or phishing. Every day we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. In addition, we use multiple antivirus engines in Gmail, Google Drive, servers, and workstations to help identify malware. In your Google Cloud environment, you can use Chronicle and VirusTotal to monitor and respond to many types of malware. -Google Cloud Threat Intelligence for Chronicle is a team of threat researchers who develop threat intelligence for use with Chronicle. -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. Refer to our security whitepaper for more information. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image. Secure Service Deployment We use cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand. Refer to our infrastructure security page for more information. Google's internal vulnerability management process actively scans for security threats across all technology stacks. This	N/A Access and Site Controls (Cloud Data Processing Addendum) Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

	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 Te 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 security whitepaper for more information. Google has a dedicated security team, which includes some of the world's foremost experts in information security, application security, cryptography, and network security. This team maintains our defense systems, develops security review processes, builds security infrastructure, and implements our security policies. The team actively scans for security threats using commercial and custom tools. The team also conducts penetration tests and performs quality assurance and security reviews. Members of the security team review security plans for our networks and services, and they provide project-specific consulting services to our product and engineering teams. The security team monitors for suspicious activity on our networks and addresses information security threats as needed. The team also performs routine security evaluations and audits, which can involve engaging outside experts to conduct regular security assessments.	N/A

	Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance, including: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS 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. Refer to our security whitepaper for more information. The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
13.3.11. The agreement must specify whether sub-contracting is permitted by the CSP directly or via other parties, and if so, what types of sub-contracting under which conditions.	Refer to our commentary on Clause 12.1.2.	
13.3.12. The agreement must contain provisions regarding the management of incidents by the CSP, including the obligation for the CSP to report to the Entity without undue delay incidents that have affected the operation of the Entity's contracted service.	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.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 Service Health 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	Data Incidents (Cloud Data Processing Addendum) Significant Developments

	dashboard, configurable alerts, exportable logs with Cloud Logging. Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. 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).	
13.3.13. The agreement must contain provisions regarding digital forensic evidence generation, including whether the original copies of forensic evidence will be utilized or a copy with a chain of custody. The chain of custody pre-requisites should be communicated and stated in the contract.	This is a customer consideration.	N/A
13.3.14. The agreement must address e-discovery costs and forensics requirements including cost and response times.	Refer to your Google Cloud Financial Services contract. Prices and fee information are also publicly available on our SKUs page. Refer to our Pricing page for more information.	Payment Terms
13.4. An Entity must receive official QCB approval prior to signing any Material Arrangement(s), or to any material modification of an existing one.	This is a customer consideration.	N/A
13.5. An Entity's contract with the CSP must include clauses that ensures data confidentiality, availability and integrity at all times, depending on the nature of service being provided by the CSP.	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers.	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

	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: Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on	

	behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: Security best practices Security use cases Security blueprints	
14. Post Outsourcing Implementation Review		
14.1. Prior to signing the contract, an Entity must plan and schedule an initial post outsourcing implementation review, set at a time after the implementation of the Material Arrangement.	This is a customer consideration.	N/A
14.2. The post outsourcing implementation review must address the following:		
14.2.1. An Entity must review the effectiveness and adequacy of the Entity's controls in monitoring the performance of the service provider and checks to ensure that the risks associated with the outsourcing activity are managed appropriately as planned.	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 Service Health 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	Ongoing Performance Monitoring

	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 Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. 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).	
14.2.2. An Entity must develop a process for CSP assessments, in collaboration with the CSP. For the initial review this must at a minimum include:		
14.2.2.1. Contract review.	This is a customer consideration.	N/A
14.2.2.2. CSP self-reported compliance review.	As part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards from around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information.	N/A
14.2.2.3. Documentation and policies review.	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)	Certifications and Audit Reports

	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.	
14.2.2.4. Available audits and assessments.	Refer to our commentary on Clause 14.2.2.3.	N/A
14.2.2.5. SLA performance.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services
14.2.2.6. Vulnerability assessments.	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 security whitepaper for more information.	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

14.2.2.7. Penetration testing.	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.	Customer Penetration Testing
14.2.3. An Entity is required to actively seek improvements in the assessment parameter's capability to supply the necessary information for effective contract monitoring. The CSP is obligated to collaborate in this endeavor.	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 Service Health 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 Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. 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).	Services
15. Compliance Assessments		
15.1. An Entity is required to conduct a full annual assessment of each Cloud Computing Arrangement.	This is a customer consideration.	N/A

15.1.1. The annual assessment must include an update and review of all the contracts in the Register, material or otherwise.	This is a customer consideration.	N/A
15.1.2. The annual assessment must report on all contracts where there has been a failure to meet contractual requirements.	This is a customer consideration.	N/A
15.1.3. The annual assessment must include information from the CSP about breaches of data, security or confidentiality in relation to the contract. A report of any such breaches at the CSP level as a whole.	Refer to our commentary on Clause 13.3.12.	
15.1.4. The annual assessment must report any changes of location by the CSP and any (approved) changes of location for the contract itself.	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.	Data Location (Service Specific Terms)
15.1.5. The annual assessment must report the CSP's financial situation.	Refer to our commentary on Clause 11.17.	
15.1.6. For Material Arrangements the assessment must cover:		
15.1.6.1. A report of performance versus the SLA.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services.
15.1.6.2. A report recording all monitoring and review of Cloud Computing Arrangements by the Entity's internal control functions, regulators, or persons employed by them, including for the purposes of supervision by QCB.	This is a customer consideration.	N/A
15.1.6.3. Any cases where the CSP was not fully co-operative with the Entity's request or those of QCB.	Google will cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Enabling Customer Compliance
15.1.6.4. A report relevant for the Entity's security function and key functions, such as reports prepared by the CSP's internal audit function.	Refer to our commentary on Clause 11.14.5.	
15.1.6.5. A report from the CSP to provide information on security measures such as: Malware protection,	Malware protection	N/A

cryptographic controls, security testing, technical compliance, KPI (Key Performance Indicators) & KRI (Key Risk Indicators	Google's malware prevention strategy begins by preventing infection using manual and automated scanners to scour our search index for websites that might be vehicles for malware or phishing. Every day we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. In addition, we use multiple antivirus engines in Gmail, Google Drive, servers, and workstations to help identify malware. In your Google Cloud environment, you can use Chronicle and VirusTotal to monitor and respond to many types of malware. -Google Cloud Threat Intelligence for Chronicle is a team of threat researchers who develop threat intelligence for use with Chronicle. -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. Refer to our security whitepaper for more information. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. Secure Machine Identity Google server machines use a variety of technologies to ensure that they are booting the correct software stack. We use cryptographic signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image. Secure Service Deployment We use cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand. Refer to our infrastructure security page for more information. Google's internal vulnerability management process actively scans for security threats across all technology stacks. This	Access and Site Controls (Cloud Data Processing Addendum) Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

	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 security whitepaper for more information. Google has a dedicated security team, which includes some of the world's foremost experts in information security, application security, cryptography, and network security. This team maintains our defense systems, develops security review processes, builds security infrastructure, and implements our security policies. The team actively scans for security threats using commercial and custom tools. The team also conducts penetration tests and performs quality assurance and security reviews. Members of the security team review security plans for our networks and services, and they provide project-specific consulting services to our product and engineering teams. The security team monitors for suspicious activity on our networks and addresses information security threats as needed. The team also performs routine security evaluations and audits, which can involve engaging outside experts to conduct regular security assessments.	N/A Services

	Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance, including: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS 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. Refer to our security whitepaper for more information. The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	
15.2. An Entity must regularly assess a CSP's compliance with the defined policy as per clause (8A).	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.	Certifications and Audit Reports
15.3. An Entity must regularly assess a CSP's compliance with the relevant requirements of this regulation.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.	Ongoing Performance Monitoring

	For example: The Service Health 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 Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. 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).	
15.4. An Entity must use the compliance to the policy as per clause (8.4) and requirements in this regulation as a criterion to renew a Cloud Computing Arrangement.	This is a customer consideration	
16. Access, Audit and Information Rights		
16.1. An Entity must aim to have enforceable contractual rights that allow an Entity to have the same access rights as if it was directly managing its Cloud Computing environment.	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.	Customer Information, Audit and Access
16.2. An Entity must ensure that QCB has the same rights to audit as if the function were not outsourced in its Cloud Computing Arrangement contracts as per clause (13.3.8).	Refer to our commentary on Clause 16.1.	N/A
16.3. An Entity must contractually have reasonable access to necessary information to assist in any investigation arising due to an incident in the cloud or audit inspection, to	Refer to our commentary on Clause 11.15.	

the extent that it does not contravene any other legal obligations.		
16.4. An Entity must ensure that there are no restrictions on the number of requests the Entity or its auditor can make to access or receive data.	Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively. You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored. There is no restriction on the number of times a customer can access its own data.	Enabling Customer Compliance Regulator Information, Audit and Access
16.5. An Entity must have access to information on controls applied on the business premises in scope of the Cloud Computing Arrangement.	Refer to our commentary on Clause 16.1	N/A
16.6. An Entity must be able to conduct an onsite visit to the relevant premises, as permitted by the CSP.	Refer to our commentary on Clause 16.1. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Customer Information, Audit and Access
16.7. An Entity must ensure that QCB has the right to access the CSP's business premises and to communicate with the CSP's subject matter experts, as permitted by the CSP.	Refer to our commentary on Clause 16.6	N/A
17. Business Continuity		
17.1. An Entity must integrate its Cloud Computing Arrangements within its Business Continuity Plans (BCP).	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.	Business Continuity and Disaster Recovery

	In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	
17.2. An Entity must detail how to switch over to the Cloud Computing disaster recovery environment and then switch back to normal cloud production within its IT disaster recovery plan.	Google recognizes the importance of regular testing in the context of operational resilience. Google runs annual, company-wide, multi-day Disaster Recovery Testing events (DiRT) to ensure that Google's services and internal business operations continue to run during a disaster. DiRT was developed to find vulnerabilities in critical systems by intentionally causing failures, and to fix those vulnerabilities before failures happen in an uncontrolled manner. DiRT tests Google's technical robustness by breaking live systems and tests our operational resilience by explicitly preventing critical personnel, area experts, and leaders from participating. All generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability. Refer to this blog post for more information about the resilience testing that Google performs as well as recommendations on how to train your first responders so they can react efficiently under pressure. You'll also find templates so you can get started testing these methods in your own organization. Firms can also request to review Google Cloud's testing results.	Business Continuity and Disaster Recovery
17.3. An Entity must assess its ability to find alternate vendors. For each CSP:		
17.4. Assess the CSP's substitutability as easy, difficult or impossible.	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.	
17.5. Identify an alternate service provider, where possible.	Refer to our commentary on Clause 17.4.	
17.6. An Entity must evaluate if the CSP's BCP against required standards to determine that the CSP has satisfactory BCP in place.	Refer to our commentary on Clause 17.1	N/A

17.7. An Entity must evaluate and satisfy itself that the interdependency risk arising from Cloud Computing Outsourcing can be adequately mitigated.	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud. In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page.	Data Export (Cloud Data Processing Addendum)
17.8. An Entity must evaluate the likelihood and impact of an unexpected disruption to the continuity of its operations.	Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including: -destruction of infrastructure required to provide the Services	N/A

	-interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures) -unavailability of key personnel -emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) -pandemics	
17.9. An Entity must proactively seek assurance on the state of the CSP's BCP preparedness.	Refer to our commentary on Clause 17.1	N/A
17.10. An Entity must integrate the CSP within its BCP test.	Refer to our commentary on Clause 17.1	N/A
17.11. An Entity must regularly update its BCP and test arrangement with the CSP to ensure their effectiveness.	Refer to our commentary on Clause 17.1	N/A
17.12. An Entity must have a defined incident response plan and develop effective crisis communication measures integrated with the CSP.	Refer to our commentary on Clause 17.1	N/A
18. Termination		
18.1. In the event of contract termination with the CSP, either on expiry or prematurely, an Entity must have the contractual right to promptly render data inaccessible at the CSP's systems, including backups.	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. Google personnel do not require access to your passwords/credentials for the services. Therefore, regulated entities do not need to revoke access privileges on termination.	N/A
18.2. Upon termination, the CSP must transfer all data from its environment to the Entity and remove it from its environment.	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. 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 Deletion on Termination (Cloud Data Processing Addendum)
18.3. An Entity must ensure that the contract clearly stipulates the situations in which the Entity must have the right to terminate the outsourcing agreement in the event of	Regulated entities can terminate our contract with advance notice for Google's material breach after a cure period, for change of control and for Google's insolvency.	Term and Termination

default, or under circumstances, including but not limited to:		
18.3.1.The CSP undergoes a change in ownership.	Refer to our commentary on Clause 18.3.	N/A
18.3.2.The CSP becomes insolvent or goes into liquidation.	Refer to our commentary on Clause 18.3.	N/A
18.3.3. The CSP goes into receivership or judicial management whether in Qatar or elsewhere.	Refer to our commentary on Clause 18.3.	N/A
18.3.4. There has been a material breach of data, security or confidentiality.	Refer to our commentary on Clause 18.3.	N/A
18.3.5.There is a demonstrable deterioration in the ability of the service provider to perform the contracted service.	Refer to our commentary on Clause 18.3.	N/A
18.3.6. The CSP proposes to move data to a new location which is unacceptable to the Entity.	Refer to our commentary on Clause 18.3.	N/A
18.4. An Entity must specify a minimum period to execute a termination provision in its agreement.	Notice periods apply for termination by both you and Google. Refer to your Google Cloud Financial Services Contract	Term and Termination
18.5. An Entity must have a legal agreement that commits the CSP to assist in the exit process so as not to unreasonably impede the exit. These must include the format and manner in which data is to be returned to the Entity, as well as support from the CSP to ensure the accessibility of the data to ensure there is a smooth transition.	Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Cloud Data Processing Addendum)
18.6. An Entity must agree on the CSP's data removal process, and the tools used for deletion of data in a manner that data is rendered irrecoverable.	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.	Deletion on Termination (Cloud Data Processing Addendum)
18.7. An Entity and the CSP must agree on the data to be returned upon termination of the Cloud Computing	Refer to our commentary on Clause 18.6	N/A

Arrangement and review whenever there are material changes to the arrangement.		
19. Exit Plan		
19.1. An Entity must develop and maintain a documented exit plan, informed by the Cloud Computing Arrangement's Materiality, which must cover and differentiate between situations where an Entity exits an outsourcing agreement.	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.	Data Export (Cloud Data Processing Addendum)
19.2. An Entity must ensure that its exit plan covers both stressed exit and managed exit.	Google recognizes that, whatever the level of technical resilience that can be achieved on Google Cloud, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: -Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. -Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. -Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on Google Cloud across other Cloud providers or on-premise. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	Data Export (Cloud Data Processing Addendum)

19.3. An Entity must have plans how it would transition to an alternative service provider (or back to the Entity) and maintain business continuity.	Refer to our commentary on Clause 19.2.	
19.4. An Entity may consider the available tools that could facilitate a stressed exit from a Cloud Computing Arrangement.	Refer to our commentary on Clause 19.2.	
PART D (OPERATIONAL SECURITY CONTROLS)		
20. Key Management Governance		
20.1. An Entity must remain accountable for the key management and ensure that the CSP is executing the applicable Sector-Specific Security Regulations and the Entity's requirements, regardless of if the keys are hosted within the CSP data center or in the Entity's premises as long as the key cryptography controls are meeting the applicable standards.	You can choose to use these encryption and key management tools provided by Google: -Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. -Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. -Customer-managed encryption keys for Cloud SQL and GKE persistent disks. - Single-Tenant Cloud HSM (STCH): A dedicated, cryptographically isolated cluster of HSM partitions. You control the cryptographic access plane via physical FIDO tokens (e.g., YubiKeys). Google operators are mathematically walled off from your cryptographic domains. -Cloud External Key Manager lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. -Key Access Justification works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to	N/A

	explicitly approve or deny providing the key using an automated policy that you set.	
20.2. An Entity must ensure that the CSP retains a record, documents and regularly monitors the implementation of the required and applicable security controls including any changes to such 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) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
20.3. An Entity must ensure that a procedure for key management access is documented and implemented.	You can choose to use these encryption and key management tools provided by Google: -Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. -Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. - Single-Tenant Cloud HSM (STCH): A dedicated, cryptographically isolated cluster of HSM partitions. You control the cryptographic access plane via physical FIDO tokens (e.g., YubiKeys). Google operators are mathematically walled off from your cryptographic domains.	N/A

	-Customer-managed encryption keys for Cloud SQL and GKE persistent disks. -Cloud External Key Manager lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. -Key Access Justification works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set.	
20.4. CSPs must limit KMS access to specific individuals for a limited time to conduct a task, based on the agreed procedure with the Entity.	Refer to our commentary on Clause 20.3.	N/A
20.5. An Entity must ensure that the principle of least privilege is adopted when granting access to the CSP.	There are a number of ways to perform effective access / configuration management using the services: Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. 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. Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. Data Boundary via Assured Workloads helps you define secure configurations and controls as code in your cloud architecture via APIs which are also expressed in some of our blueprints.	N/A
20.6. An Entity must retain the right to access all the logs generated by the procured services. This also includes	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google	N/A

having a full record of any access requests by the CSP to the KMS.	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 “Managing Google’s Access to your Data” section of our Trusting your data with Google Cloud 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. Cloud Audit Logs are encrypted at rest by default and reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail. The service is also coupled with	

	Google Cloud's Access Transparency service, which surfaces near real-time logs of Google Cloud administrator access to your systems and data.	
21. Data Protection		
21.1. An Entity must only grant service providers access to their information on a need-to-know and need-to-have basis for the purposes of the Cloud Computing Arrangement.	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.	Confidentiality
21.2. An Entity must ensure its data and information is segregated where the Cloud Computing Arrangement is using a multi-tenancy environment. Computing Arrangement:	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
21.3. An Entity must implement technical and process-based controls to protect the integrity, confidentiality of the data while the data is at rest or in motion or resident in the memory, as defined in the Sector-Specific Security Regulations.	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. 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.	N/A
21.4 An Entity must ensure that PII and financial information is processed within Qatar only.	Refer to our commentary on Clause 15.1.4.	
21.5 An Entity must receive approval from QCB prior to entering into Cloud Arrangement.	This is a customer consideration.	N/A
21.6 When using services personal data, an Entity must ensure compliance with all applicable laws or regulations relating to the protection of personal data and must require CSPs to comply with all requirements relating to the protection and processing of personal data, as applicable to such Entities.	Google will comply with all national data protection regulations applicable to it in the provision of the Services. This is addressed in the Cloud Data Processing Addendum.	Representations and Warranties
22. Cloud Security Testing		
22.1 An Entity may hire a reputable third party to assess and conduct the tests mentioned in clause (22.3) and in accordance with the Sector-Specific Security Regulation.	This is a customer consideration.	N/A
22.2 When an Entity is not permitted to conduct a certain security assessment on the cloud environment, the CSP	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular	Certifications and Audit Reports

must provide the Entity with an assessment report conducted by a reputable third party.	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.	
22.3 An Entity should regularly perform the relevant test depending on the cloud service model used in a Cloud Computing Arrangement:	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	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

	organization also fosters interaction with the industry and with the open source community. Refer to our security whitepaper for more information. Google has a dedicated security team, which includes some of the world's foremost experts in information security, application security, cryptography, and network security. This team maintains our defense systems, develops security review processes, builds security infrastructure, and implements our security policies. The team actively scans for security threats using commercial and custom tools. The team also conducts penetration tests and performs quality assurance and security reviews. Members of the security team review security plans for our networks and services, and they provide project-specific consulting services to our product and engineering teams. The security team monitors for suspicious activity on our networks and addresses information security threats as needed. The team also performs routine security evaluations and audits, which can involve engaging outside experts to conduct regular security assessments. Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance, including: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS 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. Refer to our security whitepaper for more information.	N/A

Cloud Service Model Test	IaaS	PaaS	SaaS
Architecture and infrastructure review			
Security configuration review			
Compliance review			
Application and source code testing			
Vulnerability assessment			
Penetration testing			

Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page. In addition, Google Cloud's Architecture Framework provides recommendations and describes best practices to help you design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.	N/A
Google has a dedicated security team, which includes some of the world's foremost experts in information security, application security, cryptography, and network security. This team maintains our defense systems, develops security review processes, builds security infrastructure, and implements our security policies. The team actively scans for security threats using commercial and custom tools. The team also conducts penetration tests and performs quality assurance and security reviews. Members of the security team review security plans for our networks and services, and they provide project-specific consulting services to our product and engineering teams. The security team monitors for suspicious activity on our networks and addresses information security threats as needed. The team also performs routine security evaluations and audits, which can involve engaging outside experts to conduct regular security assessments.	N/A
Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance, including: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	N/A

	Refer to our security whitepaper for more information. Google centralizes control of our software supply chain and actively secures each step of the end-to-end process. We start by maintaining separate secured copies of the source code for our dependencies and perform our own vulnerability scanning. Most of our source code is stored in a central monolithic repository, which enables employees to check code into a single location. The Google codebase simplifies source code management, in particular management of our dependencies on third-party code. A monolithic codebase also allows for the enforcement of a single choke point for code reviews. We continuously fuzz 550 of the most commonly-used open source projects. We then manage an end-to-end build, deploy, and distribution process that includes integrated integrity, provenance, and security checks. In addition: -Based on our internal security practices, Binary Authorization for Borg, we have created the SLSA framework to enable organizations to assess the maturity of their software supply chain security and understand key steps to progress to the next level. SLSA lays out an actionable path for organizations to increase their overall software supply-chain security by providing step-by-step guidelines and practical goals for protecting source and build system integrity. The SLSA framework addresses a limitation of Software Bills of Materials (SBOMs), which on their own do not provide sufficient information about integrity and provenance. -Assured OSS allows enterprise customers to directly benefit from the in-depth, end-to-end security capabilities and practices we apply to our own OSS portfolio by providing access to the same OSS packages that Google depends on. 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	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

	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 security whitepaper for more information. Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here.	Customer Penetration Testing

Shared Responsibility and Shared Fate on Google Cloud

Operating in the cloud involves a shared responsibility model, where Google Cloud and our customers both play essential roles in ensuring security and compliance. Google is responsible for the security *of* the cloud, meaning we secure the underlying infrastructure, network, and foundational services that support your operations. This includes our global data centers, hardware, software, networking, and the processes and controls for maintaining these systems.

Conversely, you, the customer, are responsible for security *in* the cloud. This entails the security of your configurations within the cloud environment, the security of your applications and data, identity and access management, network configurations, and the overall security posture of your cloud deployments. Our shared fate model signifies that we succeed together; your compliance is a collective objective, and we provide the platform and tools to assist you in achieving it. While Google Cloud furnishes a secure platform and comprehensive tools, the ultimate responsibility for achieving and maintaining compliance with the Qatar laws and regulations rests with your organization, based on your specific implementation and operational practices. For more details on this model, refer to the Shared Responsibility and Shared Fate documentation.

Partnering on Your Compliance Journey

Google Cloud is more than a technology provider; we are your partner in navigating the complexities of regulatory compliance. We are dedicated to continuously enhancing our platform and services to help financial institutions in Qatar meet evolving requirements and innovate securely.

We encourage you to explore Google Cloud's comprehensive compliance resource center to access whitepapers, compliance guides, and detailed documentation relevant to the financial sector and data governance, including the Google Cloud Trust Center, Security section, Geography and Regions documentation, Security Best Practices, and Privacy information. For guidance on how Google Cloud can support your journey to comply with QCB regulations, please do not hesitate to contact your Google Cloud account team. We are here to help you build and operate secure, compliant, and transformative solutions in the cloud.