



Malaysian Financial Services Regulations: A Guide for Institutions Using Google Cloud



Table of Contents

| | |
|---|-----------|
| Abstract | 3 |
| Google Cloud's Commitment to Security and Compliance | 3 |
| Key Regulations to Consider for Cloud Adoption | 4 |
| BNM Regulations | 4 |
| Underpinning consumer data protection | 4 |
| Enabling Your Compliance | 4 |
| Addressing shared aspects of the regulations | 5 |
| Governance Framework and Accountability | 5 |
| Risk Assessment and Due Diligence | 5 |
| Data Ownership and Protection | 6 |
| Operational Resilience, Business Continuity and Disaster Recovery | 7 |
| Regulatory Oversight and Contractual Obligations | 8 |
| Compliance with Risk Management in Technology (RMiT) and Outsourcing regulations in the context of Google Cloud | 8 |
| Risk Management in Technology (RMiT) - Section 10 | 9 |
| Outsourcing - Sections 9, 10 and 11 | 25 |
| Shared Responsibility and Shared Fate on Google Cloud | 42 |
| Partnering on Your Compliance Journey | 42 |

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of July 2025 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

Malaysia's financial sector operates under stringent regulations designed to ensure cyber resilience, technology risk management, and accountability when leveraging external services, such as the cloud. BNM is the key authority regulating these entities and maintaining the integrity and stability of the financial system.

Financial institutions (FI) retain ultimate accountability for all outsourced activities. This requires establishing robust governance, conducting comprehensive risk assessments, and implementing rigorous data protection protocols, including maintaining control over customer data and cryptographic keys. Google Cloud is dedicated to partnering with financial institutions, providing the secure and resilient infrastructure necessary to help you meet these regulatory expectations.

This guide synthesizes the foundational compliance requirements across key financial directives, centering on governance, risk assessment, data control, and operational resilience. Its primary purpose is to help regulated customers efficiently map these complex requirements to the robust security and compliance capabilities available on Google Cloud. By leveraging Google Cloud's secure infrastructure and integrated tools, this resource empowers you to build a robust risk governance framework. Ultimately, it is designed to accelerate your secure cloud adoption, ensuring you meet regulatory goals for IT risk management, enhanced cybersecurity, data protection, and operational continuity.

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 BNM 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 Regulations to Consider for Cloud Adoption

Malaysia's regulatory landscape for financial institutions demands rigorous adherence to robust IT governance, technology risk management, and data integrity standards, especially when leveraging third-party services like cloud computing. This rigor is intensified for customers designated as National Critical Information Infrastructure (NCII) entities, who face significantly stricter cybersecurity and cyber resilience mandates. To ensure compliance and maintain confidence in the financial sector, key regulations financial institutions must address include:

BNM Regulations

- [Risk Management in Technology \(RMiT\)](#) - This policy sets technology risk standards, treating cloud usage as outsourcing. FIs must conduct comprehensive risk assessments before adopting cloud services for critical systems, addressing inherent risks like location and multi-tenancy. FIs must retain ownership, control, and management of customer data and cryptographic keys.
- [Frequently Asked Questions on Risk Management in Technology \(RMiT\)](#) - This FAQ supplements the RMiT policy and provides useful explanations for the implementation of the policy.
- [Policy Document on Outsourcing](#) - This policy governs activities performed by third parties, including cloud services. FIs must ensure board accountability, conduct due diligence on the provider's capability and location. Contracts must grant the regulator access, protect data confidentiality, and establish robust business continuity and exit strategies.
- [Frequently Asked Questions on Outsourcing](#) - This FAQ supplements the Outsourcing Policy and provides useful explanations for the implementation of the policy.
- [Interoperable Credit Transfer Framework](#) - This framework ensures customer protection in credit transfer services. FIs must securely protect customer data by deploying preventive and detective controls. Non-banking FIs must obtain the Bank's prior written approval before entering a third-party arrangement for the retention or storage of customer data related to credit transfer services.
- [Clarification and Frequently Asked Questions on the Interoperable Credit Transfer Framework](#) - This clarification requires non-banking FIs to obtain prior written approval from the Bank to engage third parties for storing sensitive customer data for credit transfer transactions. The FI must ensure the provider's security controls and governance are robust and manage country risk arising from offshore arrangements.
- [Management of Customer Information and Permitted Disclosures Policy](#) - This sets out BNM's requirements and expectations of financial institutions' measures and controls in handling customer information.

Underpinning consumer data protection

- [Personal Data Protection Act \(Act A1727\)](#) - The PDPA requires financial institutions to be fully accountable for customer data, requiring them to implement robust security and adhere to all seven data protection principles, including getting explicit consent and limiting data retention.

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 BNM regulations generally place significant emphasis on key aspects of governance, risk assessment and due diligence on external service providers, data ownership and protection, operational resilience, and regulatory oversight and contractual obligations. Google Cloud offers a comprehensive set of services and features that directly align with these core domains, enabling you to address the regulations' mandates effectively.

Addressing shared aspects of the regulations

Governance Framework and Accountability

Financial institutions must establish robust cloud governance, ensuring the board and senior management retain ultimate accountability for all outsourced cloud activities and risks. This requires integrating cloud risk management into the existing Technology Risk Management Framework (TRMF) and Cyber Resilience Framework (CRF) of financial institutions. Internal policies must articulate usage criteria commensurate with criticality. The FI must maintain sufficient internal capacity and skilled resources to oversee the service provider effectively.

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 Assessment and Due Diligence

FIs must conduct comprehensive risk assessments before adopting cloud services for critical systems, addressing inherent risks like multi-tenancy, vendor lock-in, and infrastructure location. Due diligence must scrutinize the provider's competency, security controls, and management of specific risks (e.g., data leakage, geo-political risks, vendor lock-in). NCII entities must also conduct cyber security risk assessments and audits in

accordance with a specific set of requirements. This ensures risks are proportional to the FI's risk appetite.

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, 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](#).

Data Ownership and Protection

FIs must ensure the confidentiality and integrity of data residing in the cloud by implementing appropriate safeguards. They must retain ownership and control of customer data and all relevant cryptographic keys, ideally independent of the cloud provider. Data must be logically segregated from other clients, and access controls for the cloud management plane must be strong, employing multi-factor authentication and the principle of "least privilege".

Google Cloud provides a robust suite of services designed to facilitate comprehensive data governance, ensure strong data protection, and enable precise encryption controls for responsible data processing.

- **Encryption Control and Flexibility:** Encryption is a core component of Google Cloud's security model. While we secure your data at rest and in transit by default, you maintain granular control over your encryption options to meet specific compliance mandates. We offer a comprehensive continuum of key management choices, including those that allow you to generate, store, and rotate your own keys. To align your security goals with the best solution—be it Google-managed keys or customer-managed keys (CMEK) or customer-supplied keys (CSEK)—please refer to our dedicated [Choosing an Encryption Option](#) page.
- **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, to help customers [comply with Malaysia's Personal Data Protection Act](#).

- **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). [Data Security Posture Management \(DSPM\)](#) allows you to visualise data resources by sensitivity and location, secure the access with advanced data controls, and reduce overall cloud data risks.
- **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.
- **AI privacy:** In deploying AI that addresses both user needs and broader responsibilities, while safeguarding user safety, security, and privacy, Google Cloud has a long-standing commitment to [GDPR compliance](#), and we incorporate privacy-by-design and default from the beginning. Google Cloud provides clear disclosures and [commitments](#) regarding access to a customer's data. We also enable certain AI/ML services to be configured to meet [data residency requirements](#) as noted in our [Service Terms](#). More detail can be found in our [Generative AI, privacy and Google Cloud](#) whitepaper.

Operational Resilience, Business Continuity and Disaster Recovery

FIs must maintain strong recovery capabilities, ensuring backup and restoration procedures cover cloud services and are tested periodically. The Cyber Incident Response Plan (CIRP) and Business Continuity Plan (BCP) must be extended to manage adverse cloud scenarios. FIs must establish a robust and documented exit strategy during the planning phase, detailing alternative providers and ensuring data portability capabilities to facilitate an orderly transition if the arrangement fails or terminates.

Google Cloud enables customers to lead their operational resilience and business continuity planning by providing the following:

Customer Control: Region Selection for Operational Resilience

- You maintain control over where your data at rest is stored by selecting the specific Google Cloud region or multi-region for your resources, as detailed on our [Global Locations page](#). This capability allows you to deploy your electronic systems and store your data within Malaysia or other suitable regions, supporting data residency requirements and aligning with your business continuity and disaster recovery (DR) requirements. Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page.

Security and Resilience of the Cloud Infrastructure (Google-Managed Controls)

Google manages the security and resilience of our core infrastructure, encompassing the hardware, software, networking, and facilities that support the Services. This includes:

- **Encryption and Data Location:** All data stored in Google Cloud is encrypted at rest and in transit. We proactively provide [encryption at rest](#) (enabled by default with no additional action required) and [encryption in transit](#) (encrypting and authenticating all data when it moves outside Google's physical boundaries). You retain control over your data's location, and for particular services, you can configure data residency policies to ensure data remains within designated geographic boundaries. For supported services, you can also encrypt data in-use with Confidential Computing technologies.
- **Operational Resilience:** Google achieves disaster recovery (DR) and operational resilience through continuous, automated disaster readiness and recovery for all Google's systems and data. Our [SOC 2 report](#) attests to the design and operating effectiveness of controls related to security, availability, processing integrity, confidentiality, and privacy.

- **Data Incident Response:** Google will notify you of data incidents promptly and without undue delay. Our [notification](#) describes the nature of the incident, impacted resources, recommended customer actions, and contact details for more information, assisting customers with their own incident response.
- **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.
- **Google Cloud's Compliance with the Personal Data Protection Act (PDPA):** You can also leverage [Google Cloud's whitepaper on PDPA \(Malaysia\)](#) which would help you understand the PDPA and how Google Cloud implements data privacy and security capabilities to store, process, maintain, and secure customer data in a way that aids customers in meeting their PDPA obligations.

Customer-Configured Cybersecurity and Incident Management (Features in the Cloud)

You define the security measures for your data and applications within the cloud. To enhance your cybersecurity, operational continuity, and incident management capabilities, Google offers a wide range of security products and services for you to configure:

- **Operational Resilience & DR Guidance:** We provide guidance on how you can leverage Google Cloud's inherent reliability features (like zones, regions, and location-scoped resources) and architectural best practices to build robust DR solutions for your cloud infrastructure, as further detailed in our [strengthening operational resilience](#) whitepaper.
- **Security Command Center (SCC):** Provides a centralized platform for managing security and risk across your cloud environment, integrating vulnerability detection, compliance monitoring, and security posture management.
- **Google Cloud Armor:** Offers robust, global protection against DDoS attacks and Web Application Firewall (WAF) services, helping ensure the availability and security of your internet-facing applications.
- **Google Security Operations:** Unifies security operations with AI-powered analytics to accelerate threat detection, investigation, and response, ultimately strengthening your security posture and incident management capabilities.
- **Google Threat Intelligence & Mandiant:** Capabilities that leverage Google's vast security expertise to provide actionable insights for proactive defense, supplemented by strategic services like cyber defense transformation and incident response from Mandiant.
- **reCAPTCHA Enterprise:** Protects websites and applications from fraudulent activity and spam by distinguishing between human users and bots.

Regulatory Oversight and Contractual Obligations

Outsourcing agreements must contractually grant the financial institution, its external auditors, and the regulator (Bank Negara Malaysia) direct, timely, and unrestricted access to all relevant systems, information, and documents, including the right to conduct on-site supervision. FIs must adhere to mandatory consultation (for first-time critical cloud adoption) and notification requirements, submitting comprehensive risk reports and management confirmations of readiness.

Google's contractual commitments in the [Cloud Data Processing Addendum](#) apply to all customer data under your account. To enable you to comply with your regulatory oversight requirements and contractual obligations, we provide:

- **Customer's Audit Rights:** Regulated entities always retain the right to conduct an audit. Google offers regulated entities certifications and audit reports in addition to (and not instead of) information, audit and access rights.
- **Supervisory Authorities of Regulated Entities:** 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. 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.

- **Contract Compliance Management:** If Google’s performance of the Services does not meet the [Google Cloud Platform Service Level Agreements](#) regulated entities may claim service credits. Regulated entities may terminate our contract with advance notice for Google’s material breach after a cure period, for change in control or for Google’s insolvency.

Compliance with Risk Management in Technology (RMiT) and Outsourcing regulations in the context of Google Cloud

The RMiT specifies the technical risk and cyber resilience framework for using technology, treating cloud services as a form of outsourcing that must integrate with the Outsourcing policy's contractual and governance requirements. Market insights indicate that both RMiT and Outsourcing policies are important for navigating the mandatory consultation and approval process with BNM prior to the first-time adoption of public cloud for critical systems. As such, we provide further guidance¹ on how Google Cloud can help you address the applicable requirements under these regulations:

Risk Management in Technology (RMiT) - Section 10 and Appendix 10

| # | Framework Reference | Google Cloud Commentary |
|---|---|---|
| 10 Technology Operations Management details the requirements for securely operating technology systems, covering the entire lifecycle from project and system development, resilience (Data Centre and Network), Cryptography, Access Control, and Patch Management, with a crucial focus on Third Party Service Provider Management. | | |
| 1 | 10 Technology Operations Management | |
| 2 | Cryptography | |
| 3 | S 10.16 A financial institution must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. This policy, at a minimum, shall address requirements for: | |
| 4 | (a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation; | <p>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.</p> <p>(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:</p> <p>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.</p> <p>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.</p> <p>Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage,</p> |

¹ To ensure comprehensive compliance, it is the financial institution's responsibility to understand and meet all applicable regulatory requirements beyond those outlined here.

| # | Framework Reference | Google Cloud Commentary |
|---|---|---|
| | | and rotation. |
| 5 | (b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction; | Refer to row 4. |
| 6 | (c) the periodic review, at least every three years, of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols; and | 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. |
| 7 | (d) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise. | Refer to row 4. |
| 8 | S 10.18 A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | <p>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding data center and network security and data security.</p> <p>The security of a cloud service consists of two key elements:</p> <p>(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.</p> <p>Given the one-to-many nature of our service, Google provides the same robust security for all our customers.</p> <p>Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis.</p> <p>More information is available at: 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.</p> <p>(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.</p> <p>(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:</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | | <p>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.</p> <p>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.</p> <p>(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.</p> <p>(c) Security resources You can choose to use these encryption and key management tools provided by Google:</p> <ul style="list-style-type: none"> -Cloud Key Management is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. It also 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. -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. |
| 9 | Data Centre Resilience | |
| 10 | Data Centre Infrastructure | |
| 11 | S 10.21A financial institution must specify the resilience and availability objectives of its data centres which are aligned with its business needs. The network infrastructure must be designed to be resilient, secure and scalable. Potential data centre failures or disruptions must not significantly degrade the delivery of its financial services or impede its internal operations. | <p>Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 12 | S 10.22 A financial institution must ensure production data centres are concurrently maintainable. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment. | <p>Google's global scale infrastructure is designed to provide security through the entire information processing lifecycle. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators.</p> <p>Our infrastructure security page describes the security of Google's infrastructure in progressive layers starting from the physical security of our data centers, continuing on to how the hardware and software that underlie the infrastructure are secured, and finally, describing the</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| | | <p>technical constraints and processes in place to support operational security.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 13 | S 10.23 In addition to the requirement in paragraph 10.22, large financial institutions are also required to ensure recovery data centres are concurrently maintainable. | <p>Refer to row 12 for information about Google's global infrastructure scale.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 14 | S 10.24 A financial institution shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area. A financial institution must also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure. A financial institution must also ensure adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults and indicators of potential issues. | <p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>Google's business continuity plan describes Google's business continuity and disaster recovery strategy, methodology, and testing programs. The business continuity plan is designed to cover key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware.</p> <p>Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> |
| 15 | S 10.25 A financial institution is required to appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA) and set proportionate controls aligned with the financial institution's risk appetite. The assessment must consider all major risks and determine the current level of resilience of the production data centre. A financial institution must ensure the assessment is conducted at least once every three years or whenever there is a material change in the data centre infrastructure, whichever is earlier. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.22 to 10.24 have been adhered to. For data centres managed by third party service providers, a financial institution may rely on independent third party assurance reports provided such reliance is consistent with the financial institution's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment. | <p>Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:</p> <ul style="list-style-type: none"> -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 <p>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.</p> |
| 16 | Data Centre Operations | |
| 17 | S 10.26 A financial institution must ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, | <p>When using Google Cloud services, customers hand off the bulk of their capacity planning to Google. You can scale up and scale down your VM instances as needed. In addition, customers can choose to use Cloud Load Balancing which provides scaling, high availability, and traffic</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | central processing unit (CPU) power, memory and network bandwidth. A financial institution shall involve both the technology stakeholders and the relevant business stakeholders within the financial institution in its development and implementation of capacity management plans. | management for your internet-facing and private applications. Refer to our Capacity Management with Load Balancing page for more information. |
| 18 | S 10.27 A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services ¹¹ . These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | <p>You can monitor Google’s performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <p>The Service Health Dashboard provides status information on the Services.</p> <p>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.</p> <p>Google Cloud Monitoring 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.</p> <p>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).</p> |
| 19 | S 10.28 A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity ¹² . In the case where vendors’ or programmers’ access to the production environment is necessary, these activities must be properly authorised and monitored. | This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security and access. |
| 20 | S 10.29 A financial institution must establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions. | Refer to row 19 about Google’s commitments to protect your data, security and access. |
| 21 | S 10.30 A financial institution is required to undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times. A financial institution must also maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes. Backup | Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| | media must be stored in an environmentally secure and access-controlled backup site. | |
| 22 | S 10.32 Where there is a reasonable expectation for immediate delivery of service to customers or dealings with counterparties, a financial institution must ensure that the relevant critical systems are designed for high availability with a cumulative unplanned downtime affecting the interface with customers or counterparties of not more than 4 hours on a rolling 12 months basis and a maximum tolerable downtime of 120 minutes per incident. | <p>Refer to row 11-12 for information about Google's global infrastructure scale.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 23 | Network Resilience | |
| 24 | S 10.33 A financial institution must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans. | <p>Refer to row 11-12 for information about Google's global infrastructure scale.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 25 | S 10.34 A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats. | <p>Refer to row 11-12 for information about Google's global infrastructure scale.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 26 | S 10.35 A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies. | <p>Refer to row 18 for information about how you can monitor Google's performance of the Services you use (including the SLAs),</p> |
| 27 | S 10.36 A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data. | <p>Confidentiality Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> <p>Integrity</p> <p>Data integrity refers to the accuracy and consistency of data throughout its lifetime. Customers need to know that information will be correct and won't change in some unexpected way from the time it's first recorded to the last time it's observed.</p> <p>Given the different ways data can be lost, there is no silver bullet that guards against the many combinations of failure modes. As such, Google employs a defense in depth strategy that comprises multiple layers, with each successive layer of defense conferring protection from progressively less common data loss scenarios.</p> <p>More information on data integrity can be found on our Site Reliability Engineering page.</p> <p>Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access. Google also maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.</p> <p>Availability</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| | | <p>Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. In addition, Google maintains policies and procedures to ensure consideration of availability throughout the entire Customer engagement.</p> <p>Google provides customers with uptime availability metrics and industry standard audit reports and certifications. Google maintains a dashboard for service availability information and service issues: https://status.cloud.google.com/.</p> |
| 28 | S 10.37 A financial institution must establish and maintain a network design blueprint identifying all of its internal and external network interfaces and connectivity. The blueprint must highlight both physical and logical connectivity between network components and network segmentations. | Refer to our Cloud networking page for information on best practices and examples to assist with networking on Google Cloud. |
| 29 | S 10.38 A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years. | <p>Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.</p> <p>Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources.</p> <p>Cloud Audit Logs help your security teams maintain audit Cloud Audit Logs overview trails in Google Cloud and view detailed information about Admin activity, data access, and system events.</p> <p>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.</p> <p>In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools:</p> <p>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).</p> <p>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.</p> |
| 30 | S 10.39 A financial institution must implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the financial institution from other entities within the group. | To keep data private and secure, Google logically isolates each customer's data from that of other customers. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| 31 | <p>S 10.40 A financial institution is required to appoint a technically competent external service provider to carry out regular network resilience and risk assessments (NRA) and set proportionate controls aligned with its risk appetite. The assessment must be conducted at least once in three years or whenever there is a material change in the network design. The assessment must consider all major risks and determine the current level of resilience. This shall include an assessment of the financial institution's adherence to the requirements in paragraphs 10.33 to 10.39. The designated board-level committee must deliberate the outcome of the assessment.</p> | <p>This is a customer consideration.</p> <p>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:</p> <p>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.</p> <p>Information about Google's approach to risk management is available in Google's certifications and audit reports.</p> <p>Financial statements You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page.</p> <p>Audit Reports Google recognizes that regulated entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Google commits to comply with the following key international standards during the term of our contract with you:</p> <p>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</p> <p>You can review Google's current certifications and audit reports at any time.</p> |
| 32 | <p>Third Party Service Provider Management</p> | |
| 33 | <p>S 10.42 A financial institution must conduct proper due diligence on the third party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services.</p> | <p>Refer to row 31 for information that can help you conduct due diligence on Google.</p> |
| 34 | <p>In addition, an assessment shall be made of the third party service provider's capabilities in managing the following specific risks—</p> | |
| 35 | <p>(a) data leakage such as unauthorised disclosure of customer and counterparty information;</p> | <p>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.</p> <p>Refer to row 18 for information about Google's access transparency and access approvals.</p> <p>Google recognizes the importance of managing service disruptions. We do our own planning for our services. You can also use our services in your own business continuity and contingency planning. Refer to row 14 for information about Google's business continuity.</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|---|
| 36 | (b) service disruption including capacity performance; | <p>Google will implement a disaster recovery plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own disaster recovery planning is available in our Disaster Recovery Planning Guide</p> |
| 37 | (c) processing errors; | <p>Customers can use Error Reporting which aggregates and displays errors produced in your running cloud services. Using the centralized error management interface, you can find your application's top or new errors so that you can fix the root causes faster.</p> |
| 38 | (d) physical security breaches; | <p>Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Service Health Dashboard.</p> <p>In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.</p> |
| 39 | (e) cyber threats; | <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 40 | (f) over-reliance on key personnel; | <p>You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Although Google personnel manage and maintain the hardware, software, networking and facilities that support the Services, given the one-to-many nature of the services, there is no single Google personnel dedicated to delivering the services to an individual customer.</p> <p>Regulated entities can use the following functionality to control the Services:</p> <ul style="list-style-type: none"> • Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. • gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. • Google APIs: Application programming interfaces which provide access to Google Cloud. |
| 41 | (g) mishandling of confidential information pertaining to the financial institution or its customers in the course of transmission, processing or storage of such information; and | <p>Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.</p> |
| 42 | (h) concentration risk. | <p>Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our 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.</p> <p>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | | <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>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.</p> |
| 43 | S 10.43 A financial institution must establish service-level agreements (SLA) when engaging third party service providers. At a minimum, the SLA shall contain the following: | |
| 44 | (a) access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution. This shall include access to any record, file or data of the financial institution, including management information and the minutes of all consultative and decision-making processes; | <p>Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and supervisory authorities, and both their appointees. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.</p> <p>These rights apply regardless of the service location. Nothing in our contract is intended to impede or inhibit the supervisory authority's ability to audit our services effectively.</p> |
| 45 | (b) requirements for the service provider to provide sufficient prior notice to financial institutions of any sub-contracting which is substantial; | <p>Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support.</p> <p>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:</p> <ul style="list-style-type: none"> provide information about our subcontractors; provide advance notice of changes to our subcontractors; and give regulated entities the ability to terminate if they have concerns about a new subcontractor. <p>Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights, and security requirements).</p> |
| 46 | (c) a written undertaking by the service provider on compliance with secrecy provisions under relevant legislation. The SLA shall further clearly provide for the service provider to be bound by confidentiality provisions stipulated under the contract even after the engagement has ended; | <p>The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page.</p> <p>Google will comply with all laws and regulations applicable to it in the provision of the Services.</p> |
| 47 | (d) arrangements for disaster recovery and backup capability, where applicable; | Refer to Row 36 for information on Google's ability to provide disaster recovery and business continuity. |
| 48 | (e) critical system availability; and | The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page. |
| 49 | (f) arrangements to secure business continuity in the event of exit or termination of the service provider. | <p><u>Taking over activities organized by IT Service Provider</u></p> <p>Google will enable you to access and export your data throughout the duration of our contract and during a post-termination transition term. You can export your data from the Services in a number of industry</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|---|
| | | <p>standard formats. For example:</p> <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>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.</p> <p>Termination Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority.</p> <p>In addition, Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract.</p> |
| 50 | S 10.44 A financial institution must ensure its ability to regularly review the SLA with its third party service providers to take into account the latest security and technological developments in relation to the services provided. | The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page. |
| 51 | S 10.45 A financial institution must ensure its third party service providers comply with all relevant regulatory requirements prescribed in this policy document. | Google will comply with all laws and regulations applicable to it in the provision of the Services. |
| 52 | S 10.46 A financial institution must ensure data residing in third party service providers are recoverable in a timely manner. The financial institution shall ensure clearly defined arrangements with the third party service provider are in place to facilitate the financial institution's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident. | <p>Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Service Health Dashboard.</p> <p>In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.</p> |
| 53 | S 10.47 A financial institution must ensure the storage of its data is at least logically segregated from the other clients of the third party service provider. There shall be proper controls over and periodic review of the access provided to authorised users. | Refer to row 30. |
| 54 | S 10.48 A financial institution must ensure any critical system hosted by third party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third party service provider. | <p>Refer to Row 36 for information on Google's ability to provide disaster recovery and business continuity.</p> <p>Refer to Row 49 for more information about how our Services support exit.</p> |
| 55 | Cloud Services | |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| 56 | S 10.49 A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. | Refer to row 31 for information that can help you conduct due diligence on Google. |
| 57 | The assessment must specifically address risks associated with the following: | |
| 58 | (a) sophistication of the deployment model; | <p>Google provides tools to help you manage your assets on our services. For example:</p> <p>Cloud Asset Inventory allows you to view, monitor, and analyze all your Google Cloud and Anthos assets across projects and services. Not only can you export a snapshot of your entire inventory at any point of time, you can also get real-time notifications on asset config changes.</p> <p>Cloud Data Loss Prevention helps classify your data on or off cloud giving you the insights you need to ensure proper governance, control, and compliance.</p> <p>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.</p> <p>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.</p> |
| 59 | (b) migration of existing systems to cloud infrastructure; | Refer to row 49 for information about how Google supports migrating workloads. |
| 60 | (c) location of cloud infrastructure including potential geo-political risks and legal risks that may impede compliance with any legal or regulatory requirements; | <p>To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities.</p> <ul style="list-style-type: none"> Information about the location of Google's facilities and where individual GCP services can be deployed is available here. Information about the location of Google's subprocessors' facilities is available here. <p>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:</p> <ul style="list-style-type: none"> The same robust security measures apply to all Google facilities, regardless of country / region. Google makes the same commitments about all its subprocessors, regardless of country / region. <p>Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s).</p> <p>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency.</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | | operational transparency, and privacy for customers on Google Cloud Whitepaper . |
| 61 | (d) multi-tenancy or data co-mingling; | Refer to Row 34 for information about Google's logical isolation of customer data. |
| 62 | (e) vendor lock-in and application portability or interoperability; | Refer to Row 30 for information about portability and operability in Google. |
| 63 | (f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection; | Refer to row 58 for information on how to manage your assets in our services. |
| 64 | (g) exposure to cyber-attacks via cloud service providers; | <p>Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities.</p> <p>Refer to Row 8 for information about the security of the services, including information on encryption of data at rest and in transit.</p> |
| 65 | (h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination; | <p>Refer to Row 49 for information about how our Services support exit.</p> <p>Deletion On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud whitepaper.</p> |
| 66 | (i) demarcation of responsibilities, limitations and liability of the service provider; and | The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract. |
| 67 | (j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis. | Google will comply with all laws, regulations and binding regulatory guidance applicable to it in the provision of the Services. |
| 68 | G 10.50 For critical systems hosted on public cloud, a financial institution should consider common key risks and control measures as specified in Appendix 10. A financial institution that relies on alternative risk management practices that depart from the measures outlined in Appendix 10 should be prepared to explain and demonstrate to the Bank that these alternative practices are at least as effective as, or superior to, the measures in Appendix 10. | Refer to commentary on Appendix 10 below. |
| 69 | Access Control | |
| 70 | S 10.52 A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems. | <p>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security, use, incidents, access and retention. Google will ensure its employees comply with Google's security measures.</p> <p>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.</p> <p>There are a number of ways to integrate our services with your systems and to perform effective access management.</p> <p>Integration</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|---|
| | | <ul style="list-style-type: none"> • Cloud Console allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage. • Google APIs allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language. <p>Access management</p> <ul style="list-style-type: none"> • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. • Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. • Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. • Google provides a wide variety of MFA verification methods to help protect your user accounts and data. Refer to our Authentication methods for more information. |
| 71 | G 10.53 In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: | |
| 72 | (a) adopt a “deny all” access control policy for users by default unless explicitly authorised; | Google restricts access based on need-to-know and job function. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. |
| 73 | (b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; | Refer to row 72 for information about access management in Google. |
| 74 | (c) employ time-bound access rights which restrict access to a specific period including access rights granted to service providers; | Refer to row 72 for information about access management in Google. |
| 75 | (d) employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as: (i) system development and technology operations; | Refer to Row 40 for information about how you operate the services independently without action by Google personnel. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| | (ii) security administration and system administration; and (iii) network operation and network security; | |
| 76 | (e) employ dual control functions which require two or more persons to execute an activity; | Refer to Row 40 for information about how you operate the services independently without action by Google personnel. |
| 77 | (f) adopt stronger authentication for critical activities including for remote access; | Refer to Row 70 for information about authentication. |
| 78 | (g) limit and control the use of the same user ID for multiple concurrent sessions; | Customers can utilize Cloud Run to manage concurrency settings. |
| 79 | (h) limit and control the sharing of user ID and passwords across multiple users; and | Refer to Row 70 for information about ways to integrate our services with your systems and to perform effective access management. |
| 80 | (i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs. | Refer to Row 70 for information about authentication. |
| 81 | S 10.54 A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern). | Refer to Row 70 for information about authentication. |
| 82 | S 10.55 A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created. | Refer to Row 70 for information about authentication. |
| 83 | G 10.56 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents. | Refer to Row 70 for information about authentication. |
| 84 | S 10.58 A financial institution must establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated. | Refer to Row 70 for information about authentication. |
| 85 | S 10.59 A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must | Refer to Row 35 for information about Google's internal data access processes, including logs, access transparency and access approval in Google. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| | be maintained for at least three years and regularly reviewed in a timely manner. | |
| 86 | S 10.60 In fulfilling the requirement under paragraph 10.59, large financial institutions are required to— | |
| 87 | (a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and | Refer to Row 70 for information about authentication. Refer to Row 35 for information about Google’s internal data access processes, including logs, access transparency and access approval in Google. |
| 88 | (b) deploy automated audit tools to flag any anomalies. | Refer to Row 70 for information about authentication. Refer to Row 35 for information about Google’s internal data access processes, including logs, access transparency and access approval in Google. |
| 89 | Appendix 10 Part A | |
| 90 | 4. Access to cloud service providers’ certifications A financial institution should review their cloud service providers’ certifications prior to entering into any cloud arrangement or contract with such cloud service providers. At a minimum, a financial institution should: | |
| 91 | (a) Seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider’s action plans for mitigating any noncompliance; and | 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: 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 Google’s approach to risk management is available in Google’s certifications and audit reports. <u>Financial statements</u> You can review Google’s financial status and audited financial statements on Alphabet’s Investor Relations page. <u>Audit Reports</u> Google recognizes that regulated entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. 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. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| 92 | (b) Obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. The financial institution's risk assessment should address all the requirements and guidance as stipulated in the Cloud Services section (paragraphs 10.49 to 10.51) of this policy document and paragraph 11 of the Bank's policy document on Outsourcing which sets out provisions on outsourcing involving cloud services. | Refer to the item above. |
| 93 | 6. Oversight over cloud service providers A financial institution should ensure effective oversight over cloud service providers taking into account the fact that the cloud service providers may engage subcontractor(s) to provide cloud services. This includes, at a minimum, the following: | |
| 94 | (a) establish and define a continuous monitoring mechanism with alignment to the enterprise outsourcing risk management framework (or equivalent) to ensure adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis; | <p>The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page.</p> <p>Google will comply with all laws and regulations applicable to it in the provision of the Services.</p> |
| 95 | (c) perform assessments of the outsourcing arrangement involving cloud service providers periodically in accordance with the financial institution's internal policy to achieve business resilience with emphasis on data security and ensure prompt notification to the Bank of the developments that may result in material impact to the financial institution (such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development) in line with the Bank's policy document on Outsourcing (Outsourcing PD), in particular, provisions relating to outsourcing of cloud services outside Malaysia including paragraphs 9, 10 and 11 of the Outsourcing PD; and | <p>Google will implement a disaster recovery plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own disaster recovery planning is available in our Disaster Recovery Planning Guide</p> <p>Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Service Health Dashboard.</p> <p>In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.</p> |
| 96 | (d) promptly review or re-perform risk assessment upon any material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development. | Refer to row 91, 94 and 95. |

Outsourcing - Sections 9, 10 and 11

| # | Framework Reference | Google Cloud Commentary |
|--|--|-------------------------|
| Section 9 outlines the requirements for financial institutions concerning the outsourcing process and the management of risks, emphasizing comprehensive due diligence on service providers. | | |
| 1 | 9 Outsourcing process and management of risks | |

| # | Framework Reference | Google Cloud Commentary |
|---|---|---|
| 2 | G 9.1 Effective management of outsourcing risk requires financial institutions to have an in-depth and holistic understanding of risks arising from outsourcing arrangements. This entails an understanding of the relationship between the financial institution and the service provider, and impact of the outsourcing arrangement to the operations of the financial institution. | 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. |
| 3 | Assessment of service provider | |
| 4 | G 9.2 Conducting a comprehensive and robust due diligence process is necessary for a financial institution to make an informed selection of service providers in relation to the risks associated with the outsourcing arrangement. | 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: 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. |
| 5 | S 9.3 A financial institution must conduct appropriate due diligence of a service provider at the point of considering all new arrangements, and renewing or renegotiating existing arrangements. The scope and depth of the due diligence process must be commensurate with the materiality of the outsourced activity. The due diligence process must cover, at a minimum - | Information about Google's approach to risk management is available in Google's certifications and audit reports. <u>Financial statements</u> You can review Google's financial status and audited financial statements on Alphabet's Investor Relations page. <u>Audit Reports</u> Google recognizes that regulated entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. 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. |
| 6 | (a) capacity, capability, financial strength and business reputation ¹² [Footnote 12] This includes an assessment that the service provider is a going concern and has strong governance structures to manage the outsourced activity throughout the duration of the arrangement. | <u>Capacity and capability</u> <ul style="list-style-type: none"> Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Google employs some of the world's foremost experts in information, application and network security. Information about Google Cloud's leadership team is available on our Media Resources page. <u>Financial strength</u> |

| # | Framework Reference | Google Cloud Commentary |
|---|--|---|
| | | <ul style="list-style-type: none"> You can review Google's audited financial statements on Alphabet's Investor Relations page. <p><u>Business reputation</u></p> <ul style="list-style-type: none"> Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about our referenceable customers 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. |
| 7 | <p>(a) risk management and internal control capabilities, including physical and IT security controls, and business continuity management¹³</p> <p>[Footnote 13] Including the ability of the service provider to respond to service disruptions or problems resulting from natural disasters, or physical or cyber-attacks, within an appropriate timeframe.</p> | <p>Google recognizes that regulated entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Google commits to comply with the following key international standards during the term of our contract with you:</p> <p>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</p> <p>You can review Google's current certifications and audit reports at any time.</p> <p><u>Business continuity management</u></p> <p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>Google's business continuity plan describes Google's business continuity and disaster recovery strategy, methodology, and testing programs. The business continuity plan is designed to cover key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware.</p> <p>Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> |
| 8 | <p>(a) the location of the outsourced activity (e.g. city and country), including primary and back-up sites;</p> | <p>Information about the location of Google's facilities and where individual GCP services can be deployed is available here.</p> |
| 9 | <p>(a) access rights of the financial institution and the Bank to the service provider;</p> | <p>Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| 10 | (a) measures and processes to ensure data protection and confidentiality; | 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. |
| 11 | (a) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement; | <p>Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support.</p> <p>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:</p> <ul style="list-style-type: none"> provide information about our subcontractors; provide advance notice of changes to our subcontractors; and give regulated entities the ability to terminate if they have concerns about a new subcontractor. <p>Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights, and security requirements).</p> |
| 12 | <p>(a) undue risks¹⁴ resulting from similar business arrangements, if any, between the service provider and the financial institution;</p> <p>[Footnote 14] For instance, concentration risk to a systemic service provider in the industry or where the service provider's fee structure or relationship with the financial institution may create potential conflict of interest issues.</p> | <p>Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our 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.</p> <p>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>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.</p> |
| 13 | (a) the extent of concentration risk to which the financial institution is exposed with respect to a single service provider and the mitigation measures to address this concentration. This does not apply to a service provider that is an affiliate and is supervised by a financial regulatory authority; and | <p>Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our 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.</p> <p>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | | <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>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.</p> |
| 14 | (a) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document. | <p>Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services.</p> <p>In addition, Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance.</p> |
| 15 | Outsourcing agreement | |
| 16 | S 9.6 An outsourcing arrangement must be governed by a written agreement that is legally enforceable. The outsourcing agreement must, at a minimum, provide for the following- | The use of the Services is governed by the Google Cloud Financial Services Contract. |
| 17 | (a) duration of the arrangement with date of commencement and expiry or renewal date; | Refer to your Google Cloud Financial Services Contract. |
| 18 | (a) responsibilities of the service provider, with well-defined and measurable risk and performance standards in relation to the outsourced activity. Commercial terms tied to the performance of the service provider must not create incentives for the service provider to take on excessive risks that would affect the financial institution; | <p><u>Performance standards</u></p> <p>The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.</p> <p><u>Commercial terms</u></p> <p>Refer to your Google Cloud Financial Services. Prices and fee information are also publicly available on our SKUs page.</p> |
| 19 | (a) controls to ensure the security of any information shared with the service provider at all times, covering at a minimum- | This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. |
| 20 | (i) responsibilities of the service provider with respect to information security; | 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. |
| 21 | (ii) scope of information subject to security requirements; | Google's security commitments in the Cloud Data Processing Addendum apply to all customer data under your account. |
| 22 | (iii) provisions to compensate the financial institution for any losses and corresponding liability obligations arising from a security | Refer to your Google Cloud Financial Services Contract. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| | breach attributable to the service provider; | |
| 23 | (iv) notification requirements in the event of a security breach; and | 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 . |
| 24 | (v) applicable jurisdictional laws; | Refer to your Google Cloud Financial Services Contract. |
| 25 | (a) use of information shared with the service provider is limited to the extent necessary to perform the obligations under the outsourcing agreement; | <p>You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. Although Google personnel manage and maintain the hardware, software, networking and facilities that support the Services, given the one-to-many nature of the services, there is no single Google personnel dedicated to delivering the services to an individual customer.</p> <p>Regulated entities can use the following functionality to control the Services:</p> <ul style="list-style-type: none"> • Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. • gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. • Google APIs: Application programming interfaces which provide access to Google Cloud. |
| 26 | (a) continuous and complete access by the financial institution to its data held by the service provider in the event of a dispute with the service provider, or termination of the arrangement; | Regulated entities may access their data on the services at any time. |
| 27 | (a) ability of the financial institution and its external auditor ¹⁵ to conduct audits and on-site inspections on the service provider and its sub-contractors, and to obtain any report or finding made in relation to the outsourced activity; | <p>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.</p> <p>Google will ensure our subcontractors comply with the information, access and audit rights we provide to regulated entities and supervisory authorities.</p> |
| 28 | (a) notification to the financial institution of adverse developments that could materially affect the service provider's ability to meet its contractual obligations; | <p>Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis.</p> <p>Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.</p> |

[Footnote 15] Including an agent appointed by the financial institution.

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | | In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper . |
| 29 | (a) measures that the service provider would take to ensure continuity of the outsourced activity in the event of an operational disruption or failure on the part of the service provider; | Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide . |
| 30 | (a) regular testing of the service provider's business continuity plans (BCP), including specific testing that may be required to support the financial institution's own BCP testing, and a summary of the test results to be provided to the financial institution with respect to the outsourced activity; | Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide . |
| 31 | (a) the dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant; | <p><u>Disputes</u></p> <p>Refer to your Google Cloud Financial Services Contract.</p> <p><u>Remedies</u></p> <p>If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.</p> <p><u>Indemnity</u></p> <p>Google provides regulated entities with an indemnity for certain third party claims. Refer to your Google Cloud Financial Services Contract.</p> |
| 32 | (a) circumstances that may lead to termination of the arrangement, the contractual parties' termination rights and a minimum period to execute the termination provisions, including providing sufficient time for an orderly transfer of the outsourced activity to the financial institution or another party; | <p><u>Termination</u></p> <p>Regulated entities can elect to terminate our contract for convenience with advance notice, including for Google's material breach after a cure period.</p> <p><u>Transfer</u></p> <p>Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract.</p> <p>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| | | <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>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.</p> |
| 33 | <p>(a) where relevant, terms governing the ability of the primary service provider to sub-contract to other parties. Sub-contracting should not dilute the ultimate accountability of the primary service provider to the financial institution over the outsourcing arrangement, and the institution must have clear visibility over all sub-contractors¹⁶. Therefore, the outsourcing agreement between the financial institution and primary service provider must stipulate the following:</p> <p>[Footnote 16] In this respect, the primary service provider must provide sufficient notice to the financial institution before entering into an agreement with the sub-contractor.</p> | <p>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:</p> <ul style="list-style-type: none"> • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor. |
| 34 | <p>(i) the accountability of the primary service provider over the performance and conduct of the sub-contractor in relation to the outsourcing arrangement;</p> | <p>Google will remain accountable to you for the performance of all subcontracted obligations.</p> |
| 35 | <p>(ii) the rights of the financial institution to terminate the outsourcing agreement in the event of excessive reliance on sub-contracting (e.g. where the sub-contracting materially increases the risks to the financial institution); and</p> | <p>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.</p> |
| 36 | <p>(iii) the requirement for the sub-contractor and its staff to be bound by</p> | <p>Google requires our subcontractors to meet the same high standards that we do.</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|---|--|
| | <p>confidentiality provisions even after the arrangement has ceased¹⁷; and</p> <p>[Footnote 17] See paragraph 9.9(f)</p> | <p>In particular:</p> <ul style="list-style-type: none"> • Google requires our subcontractors to 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 will ensure that all persons authorised to process customer data are under an obligation of confidentiality. • Google's confidentiality obligations survive expiry or termination of the contract. |
| 37 | (a) corresponding obligations for staff of the service provider, who are involved in the delivery of services to the financial institution's customers, to comply with similar conduct standards imposed by the Bank on the financial institution. | <p>Google will ensure its employees comply with Google's security measures and that all personnel authorized to process customer data are under an obligation of confidentiality.</p> <p>In addition, Google requires all its employees to comply with the Alphabet Code of Conduct.</p> |
| 38 | S 9.7 The outsourcing agreement must also contain provisions which– | |
| 39 | (a) enable the Bank to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity; | Regulated entities may access their data on the services at any time and may provide their supervisory authority with access. |
| 40 | (b) enable the Bank to conduct on-site supervision of the service provider where the Bank deems necessary; | 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. |
| 41 | (c) enable the Bank to appoint an independent party to perform a review of the relevant systems, information or documents of the service provider relating to the outsourced activity, where the Bank deems necessary; and | Google grants information, audit and access rights to supervisory authorities, and both their appointees. This includes a third party auditor appointed by the supervisory authority. |
| 42 | (d) allow the financial institution the right to modify or terminate the arrangement when the Bank issues a direction to the financial institution to that effect under the FSA, IFSA or DFIA, as the case may be. | Regulated entities can elect to terminate our contract for convenience with advance notice, including if directed by a supervisory authority. |
| 43 | Protection of data confidentiality | |
| 44 | G 9.8 Misuse, unauthorised or inadvertent disclosure of confidential information is a serious risk event for financial institutions. It is therefore imperative that the financial institution satisfies itself that the level of security controls, governance, policies, and procedures at the service provider are robust to protect the security and confidentiality of information shared under the outsourcing arrangement. | <p>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding data center and network security and data security.</p> <p>Security of Google's infrastructure</p> <p>The security of a cloud service consists of two key elements: Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.</p> <p>Given the one-to-many nature of our service, Google provides the</p> |

| # | Framework Reference | Google Cloud Commentary |
|---|---------------------|--|
| | | <p>same robust security for all our customers.</p> <p>Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis.</p> <p>More information is available at: 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.</p> <p>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.</p> <p>(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:</p> <p>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.</p> <p>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.</p> <p>(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.</p> <p>(c) Security resources You can choose to use these encryption and key management tools provided by Google:</p> <ul style="list-style-type: none"> -Cloud Key Management is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. It also 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. -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 |

| # | Framework Reference | Google Cloud Commentary |
|----|--|---|
| | | providing the key using an automated policy that you set. |
| 45 | S 9.9 A financial institution must ensure that appropriate controls are in place and are effective in safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, the financial institution must ensure that– | Refer to the item above. |
| 46 | (a) information disclosed to the service provider is limited to the extent necessary to provide the contracted service, and only on a need-to-know basis; | 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. |
| 47 | (b) information shared with the service provider is used only to the extent necessary to perform the obligations under the outsourcing agreement; | 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. |
| 48 | (c) all locations (e.g. city and country) where information is processed or stored, including back-up locations, are made known to the financial institution; | <p>To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities.</p> <ul style="list-style-type: none"> Information about the location of Google’s facilities and where individual GCP services can be deployed is available here. Information about the location of Google’s subprocessors’ facilities is available here. <p>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:</p> <ul style="list-style-type: none"> The same robust security measures apply to all Google facilities, regardless of country / region. Google makes the same commitments about all its subprocessors, regardless of country / region. <p>Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s).</p> <p>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.</p> |
| 49 | (d) where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are comparable to Malaysia; | 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 . |
| 50 | (e) where the service provider provides services to multiple clients, the financial institution’s information must be segregated ¹⁸ from the | To keep data private and secure, Google logically isolates each customer’s data from that of other customers. |

| # | Framework Reference | Google Cloud Commentary |
|----|--|--|
| | information of other clients of the service provider; [Footnote 18] Either logically or physically. | |
| 51 | (f) the service provider is bound by confidentiality provisions stipulated under the outsourcing agreement even after the arrangement has ceased; and | <p>Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.</p> <p>Google's confidentiality obligations survive expiry or termination of the contract.</p> |
| 52 | (g) information shared with the service provider is destroyed, rendered unusable, or returned to the financial institution in a timely and secure manner once the outsourcing arrangement ceases or is terminated. | <p><u>Deletion</u> 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.</p> <p><u>Return</u> Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> <ul style="list-style-type: none"> • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. |
| 53 | Business continuity planning | |
| 54 | G 9.10 A financial institution is responsible for ensuring that its BCP consider any operational disruptions at, or failure of, the service provider. | <p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> |
| 55 | S 9.11 A financial institution must ensure that its BCP provide for all outsourcing arrangements. The depth and comprehensiveness of the BCP must be commensurate with the materiality of the outsourcing arrangements. At a minimum, the financial institution must ensure that the BCP include probable, adverse scenarios ¹⁹ with specific action plans. The practicality of such plans must, among others, take into consideration– | <p>Google's business continuity plan is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including destruction of infrastructure required to provide the Services, interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures), unavailability of key personnel, emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake) and pandemics.</p> <p>We recognize that, whatever the level of technical resilience that can be achieved on GCP, regulated entities must plan for the scenario in which Google can no longer provide the service.</p> <p>We support such exit plans through:</p> |

| # | Framework Reference | Google Cloud Commentary |
|----|--|---|
| | <p>[Footnote 19] For instance, failure, liquidation or operational disruption of the service provider, non-performance by the service provider, unexpected termination of the outsourcing arrangement, or material deterioration in the performance of the service provider.</p> | <ul style="list-style-type: none"> • 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. • Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine. <p>Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commit to open source and common standards.</p> |
| 56 | (b) the possible need for an alternative service provider, including considerations of the limited number of service providers in the market; and | <p>Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our 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.</p> <p>In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:</p> <p>Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.</p> <p>Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine.</p> <p>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.</p> |
| 57 | (c) the degree of difficulty, cost and time required to reintegrate the outsourced activity in-house. | Refer to the item above. |
| 58 | S 9.12 In the event of a disruption, material outsourced activities must be resumed without undue delay and with minimal impact and disruptions to both business operations and the financial institution’s customers. | <p>Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it.</p> <p>In addition, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications</p> |
| 59 | S 9.13 A financial institution must, at all times, ensure that it has ready access to all its records and information at the service provider with respect to | You retain all intellectual property rights in your data. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| | the outsourced activity which would be necessary for it to operate and meet its legal and regulatory obligations. This includes scenarios where network connectivity is not available, the service provider becomes insolvent or a dispute resolution process is ongoing. | 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: <ul style="list-style-type: none"> • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner. |
| 60 | S9.14 A financial institution must periodically test its own BCP and proactively seek assurance on the state of BCP preparedness of the service provider and where relevant, alternative service providers. The intensity and regularity of the BCP testing and assessments of BCP preparedness must be commensurate with the materiality of the outsourcing arrangement. In assessing this preparedness, the financial institution must, at a minimum- | 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. |
| 61 | (a) ensure that the back-up arrangements are available and ready to be operated when necessary; | Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup |
| 62 | (b) ensure that the service provider periodically tests its BCP and provides any test reports, including any identified deficiencies, that may affect the provision of the outsourced service and measures to address such deficiencies as soon as practicable; and | 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. |
| 63 | (c) for material outsourcing arrangements, participate in joint testing with the service provider to enable an end-to-end BCP test for | 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. |

| # | Framework Reference | Google Cloud Commentary |
|---|---|---|
| | these arrangements by the financial institution. | |
| Section 10 imposes additional requirements on financial institutions for arrangements where outsourced activities or services are performed outside Malaysia. | | |
| 64 | 10 Outsourcing outside Malaysia | |
| 65 | <p>G 10.1 Outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia exposes a financial institution to additional risks (e.g. country risk). A financial institution should have in place appropriate controls and safeguards to manage these additional risks, having regard to social and political conditions, government policies, and legal and regulatory developments.</p> | <p>To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities.</p> <ul style="list-style-type: none"> Information about the location of Google's facilities and where individual GCP services can be deployed is available here. Information about the location of Google's subprocessors' facilities is available here. <p>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:</p> <ul style="list-style-type: none"> The same robust security measures apply to all Google facilities, regardless of country / region. Google makes the same commitments about all its subprocessors, regardless of country / region. <p>Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s).</p> <p>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.</p> |
| 66 | <p>S 10.2 In conducting the due diligence process, a financial institution must ensure that such assessment addresses the added dimensions of risks associated with outsourcing outside Malaysia, and the ability of the financial institution or service provider to implement appropriate responses to emerging risk events in a timely manner.</p> | <p>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:</p> <ul style="list-style-type: none"> The same robust security measures apply to all Google facilities, regardless of country / region. Google makes the same commitments about all its subprocessors, regardless of country / region. |
| 67 | <p>S 10.3 A financial institution must ensure that outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect-</p> | |
| 68 | <p>(a) the financial institution's ability to effectively monitor the service provider and execute the institution's BCP;</p> | <p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <p>The Service Health Dashboard provides status information on the Services.</p> <p>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</p> |

| # | Framework Reference | Google Cloud Commentary |
|---|--|---|
| | | <p>between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging.</p> <p>Google Cloud Monitoring 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.</p> <p>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).</p> <p>Business Continuity Planning Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>Google's business continuity plan describes Google's business continuity and disaster recovery strategy, methodology, and testing programs. The business continuity plan is designed to cover key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware.</p> <p>Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> |
| 69 | (b) the financial institution's prompt recovery of data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; and | Regulated entities may access their data on the services at any time and may provide their supervisory authority with access. These rights apply regardless of where the data are stored. |
| 70 | (c) the Bank's ability to exercise its regulatory or supervisory powers, in particular the Bank's timely and unrestricted access to systems, information or documents relating to the outsourced activity. | 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. These rights apply regardless of the service location. |
| Section 11 describes requirements for financial institutions to conduct comprehensive risk assessment and implement robust data safeguards. | | |
| 71 | 11 Outsourcing involving cloud services | |
| 72 | G 11.1 Where the outsourcing arrangement involves a cloud service provider, a financial institution should take effective measures to address risks associated with data accessibility, confidentiality, integrity, sovereignty, recoverability and regulatory compliance. This is particularly important as cloud service providers often operate a geographically dispersed computing infrastructure | This document explains how regulated entities can address their requirements whilst using Google Cloud services. |

| # | Framework Reference | Google Cloud Commentary |
|----|---|---|
| | with regional or global distribution of data processing and storage. | |
| 73 | S 11.2 In using cloud services, the inherent risks involved are similar to that of other forms of outsourcing arrangements. A financial institution that subscribes to cloud services must comply with the requirements of this policy document, and other relevant requirements on cloud services as specified by the Bank. | This document explains how regulated entities can address their requirements whilst using Google Cloud services. |
| 74 | <p>S 11.3 In relation to a financial institution's ability to conduct audits and inspections on the cloud service provider and sub-contractors pursuant to paragraph 9.6(f), the financial institution may rely on third party certification and reports made available by the cloud service provider for the audit²⁰, provided such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit.</p> <p>[Footnote 20] For the avoidance of doubt, such certifications or reports should not substitute the financial institution's right to conduct on-site inspections where necessary.</p> | <p><u>Third-party reports</u></p> <p>Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <p><u>Scope of audit</u></p> <p>Google's audit scope covers in scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope.</p> <p><u>Audit right</u></p> <p>Regulated entities always retain the right to conduct an audit. Google offers regulated entities certifications and audit reports in addition to (and not instead of) audit, access and information rights.</p> |
| 75 | S 11.4 In relation to the testing of a cloud service provider's BCP pursuant to paragraph 9.6(i), a financial institution must be able to access information on the state of robustness of the controls instituted by such cloud service providers arising from the BCP testing. | <p>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.</p> <p>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.</p> |

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 Malaysian 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 Malaysia 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](#). To accelerate your deployment, you can also leverage our pre-built resources like the [Google Cloud Security Foundations Blueprint](#) and the [Terraform Example Foundation on GitHub](#) as a starting point.

For guidance on how Google Cloud can support your journey to comply with specific BNM 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.