Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

This document is designed to help BSFIs supervised by the Bangko Sentral ng Pilipinas ("**regulated entity**") to consider The BSP Manual of Operation for Banks ("**framework**") in the context of Google Workspace and the Google Cloud Financial Services contract.

We focus on the following requirements of the framework: Section 3 of Appendix 78 of the MORB and Appendix 103 of the MORB. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	**Appendix 78 - IT RISK MANAGEMENT STANDARDS AND GUIDELINES**		
2.	**3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM**		
3.	**3.1 Risk Assessment.** Prior to entering into an outsourcing plan, the BSFI should clearly define the business requirements for the functions or activities to be outsourced, assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks. Risk assessment should take into consideration the criticality of the services to be outsourced, the capability of the technology service provider (TSP)and the technology it will use in delivering the outsourced service. Such assessment should be made periodically on existing arrangements as part of the outsourcing program and review process of the BSFI.	Google recognizes that you need to plan and execute your migration carefully. Our Migrate your organization's data to Google Workspace 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.	N/A
4.	3.2 **Service Provider Selection**. Before selecting a service provider, the BSFI should perform appropriate due diligence of the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity in relation to the services to be outsourced. The depth and formality of the due diligence performed may vary depending on the nature of the outsourcing arrangement and the BSFI's familiarity with the prospective service providers. Contract negotiation should be initiated with the service provider determined to best meet the business requirements of the BSFI.	Reputation • You can review information about Google's historic performance of the services on our G Suite Status Dashboard. • 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. Managerial skills • Information about Google Cloud's leadership team is available on our Media Resources page. • Google employs some of the world's foremost experts in information, application and network security. • Capability • 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 Google Workspace Cloud Customer page. • Information about Google Cloud's corporate history is available on Alphabet's Investor Relations page.	N/A

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct.	
5.	Due diligence undertaken during the selection process should be documented and reviewed periodically, using the most recent information, as part of the monitoring and control processes of outsourcing.	This is a customer consideration.	N/A
6.	3.3 **Outsourcing Contracts**. The contract is the legally binding document that defines all aspects of the servicing relationship and one of the most important controls in outsourcing process. It should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality and reporting. Before signing a contract, management should:	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A
7.	a. Ensure the contract clearly defines the rights and responsibilities of both parties and contains or supported by adequate and measurable service level agreements;	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract The SLAs provide measurable performance standards and remedies for the services and are available on our Google Workspace Service Level Agreement page.	Services
8.	b. Ensure contracts with related entities clearly reflect an arms-length relationship and costs and services are on terms that are substantially the same, or at least as favorable to the BSFI, as those prevailing at the time for comparable transactions with non- related third parties;	Refer to your Google Cloud Financial Services Contract. Prices and fee information are also publicly available on our Pricing page.	Payment Terms
9.	c. Choose the most appropriate pricing method for the BSFI's needs;	Refer to Row 8 above.	N/A
10.	d. Ensure service provider's physical and data security standards meet or exceed the BSFI's standards. Any breach in security should be reported by the service provider to the BSFI;	Security Standards Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • SOC 1 • SOC 2 • SOC 3	Certifications and Audit Reports

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Incident Reporting 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 whitepaper.	Data Incidents (Cloud Data Processing Addendum
11.	e. Engage legal counsel to review the contract; and	This is a customer consideration.	N/A
12.	f. Ensure the contract contains the minimum provisions required under existing Bangko Sentral rules and regulations, like access by Bangko Sentral to systems and databases outsourced, and the same does not include any provisions or inducements that may adversely affect the BSFI (i.e. extended terms, significant increases after the first few years, substantial cancellation penalties).	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.	Enabling Customer Compliance
13.	Each agreement should allow for renegotiation and renewal to enable the BSFI to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet its legal and regulatory obligations. The agreement should also acknowledge Bangko Sentral's supervisory authority over the BSFI and the right of access to information on the BSFI and the service provider.	We appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation. 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.	Enabling Customer Compliance Regulator Information, Audit and Access Customer Information, Audit and Access
14.	Some service providers may contract with third-parties in providing IT services to the BSFI. The extent to which subcontractors perform additional services should be limited to peripheral or support functions while the core services should rest with the main service provider. The BSFI should retain the ability to maintain similar control over its outsourcing risks when a service provider uses subcontractors in the course of rendering the IT-related services. Agreements should have clauses setting out the rules and limitations on subcontracting. To provide accountability, it may be beneficial for the BSFI to include a provision specifying that the contracting service provider shall remain	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	fully responsible with respect to parts of the services which were further outsourced to subcontractors. It should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights). Google will remain accountable to you for the performance of all subcontracted obligations.	
15.	An annual review of the outsourcing agreements should be performed to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies. When renegotiating contracts, the BSFI should ensure that the provider delivers a level of service that meets the needs of the institution over the life of the contract.	This is a customer consideration.	N/A
16.	3.4 **Service Level Agreement (SLA).** SLAs formalize the performance standards against which the quantity and quality of service should be measured. Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability for the outsourced activity. The BSFI should link SLA to the provisions in the contract regarding incentives, penalties and contract cancellation in order to protect themselves in the event the service provider failed to meet the required level of performance.	The SLAs provide measurable performance standards for the services and are available on our Google Workspace Service Level Agreement. If Google's performance of the Services does not meet the Google Workspace Service Level Agreements regulated entities may claim service credits.	Services
17.	Management should closely monitor the service provider's compliance with key SLA provision on the following aspects, among others:		
18.	a. Availability and timeliness of services;	The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Workspace Service Level Agreements page.	Services
19.	b. Confidentiality and integrity of data;	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. 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.	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: ● **Encryption at rest.** Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. ● **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. (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	

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
20.	c. Change control;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also control changes to your use of the services. Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services
21.	d. Security standards compliance, including vulnerability and penetration management;	Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Refer to our security whitepaper for more information.	N/A

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
22.	e. Business continuity compliance; 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.	Business Continuity and Disaster Recovery
23.	f. Help desk support.	The support services are described on our technical support services guidelines page.	Technical Support
24.	SLAs addressing business continuity should measure the service provider's contractual responsibility for backup, record retention, data protection, and maintenance and testing of disaster recovery and contingency plans. Neither contracts nor SLAs should contain any extraordinary provisions that would exempt the service provider from implementing its contingency plans (outsourcing contracts should include clauses that discuss unforeseen events for which the BSFI would not be able to adequately prepare).	Nothing in our contract or SLAs is intended to excuse Google from implementing its business continuity plan.	Business Continuity and Disaster Recovery
25.	3.5 **Ongoing Monitoring**		
26.	3.5.1 Monitoring Program. As outsourcing relationships and interdependencies increase in materiality and complexity, the BSFI needs to be more proactive in managing its outsourcing relationships. It should establish a monitoring program to ensure service providers deliver the quantity and quality of services required by the contract. The resources to support this program will vary depending on the criticality and complexity of the system, process, or service being outsourced.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring
27.	The program should employ effective mechanisms to monitor key aspects of the outsourcing relationship and the risk associated with the outsourced activity, particularly the following:		
28.	a. contract/SLA performance;	Refer to Row 26.	N/A

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
29.	b. material problems encountered by the service provider which may impact the BSFI;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Status Dashboard page.	Significant Developments
30.	c. financial condition and risk profile; and	Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page.	N/A
31.	d. business continuity plan, the results of testing thereof and the scope for improving it.	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.	Business Continuity and Disaster Recovery
32.	To increase the effectiveness of monitoring mechanisms, management should periodically classify service provider relationships to determine which service providers require closer monitoring. Relationships with higher risk classification should receive more frequent and stringent monitoring for due diligence, performance (financial and/or operational), and independent control validation reviews.	This is a customer consideration.	N/A
33.	Personnel responsible for monitoring activities should have the necessary expertise to assess the risks and should maintain adequate documentation of the process and results thereof. Management should use such documentation when renegotiating contracts as well as developing business continuity planning requirements.	Google provides documentation to explain how regulated entities and their employees can use our Google Workspace services. If a regulated entity would like more guided training, Google also provides a variety of courses and certifications.	N/A
34.	Reports on the monitoring and control activities of the BSFI should be prepared or reviewed by its senior management and provided to its Board. The BSFI should also ensure that any adverse development arising from any outsourced activity is brought to the attention of the senior management, or the Board, when warranted, on a timely basis. Actions should be taken to review the outsourcing relationship for modification or termination of the agreement.	This is a customer consideration.	N/A
35.	3.5.2. **Financial Condition of Service Providers**. The BSFI should have an on-going monitoring of the financial condition of its service providers as financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession. In the event management recognizes that the financial condition of the provider is declining or unstable, more frequent financial reviews of said provider are warranted.	Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page.	N/A
36.	3.5.3. **General Control Environment of the Service Provider**. The BSFI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their	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.	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	function. Management should restrict their access to BSFI's systems, and appropriate access controls and monitoring should be in place between the service provider's systems and the BSFI.	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Workspace resources. • Workspace Audit Logs help your security teams maintain audit trails in Google Workspace and view detailed information about Admin activity, data access, and system events. • 2-Step Verification provides a wide variety of verification methods to help protect your user accounts and data. The "Managing Google's Access to your Data" section of our Trusting your data with Google Workspace whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
37.	3.6. **Business Continuity Planning Consideration**. The BSFI should integrate the provider's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications.	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.	Business Continuity and Disaster Recovery
38.	3.7. **Compliance with Bangko Sentral Regulations**. The BSFI should ensure that appropriate up-to-date records relevant to its outsourcing arrangements are maintained in its premises and kept available for inspection by the Bangko Sentral Examiners. The outsourcing agreement should explicitly provide a clause allowing Bangko Sentral and BSFIs' internal and external auditors to review the operations and controls of the service provider as they relate 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.	Regulator Information, Audit and Access Customer Information, Audit and Access

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
39.	In addition to the general guidelines on outsourcing contracts stated in Item No. "3.3" of this Appendix, the BSFIs intending to outsource must comply with existing Bangko Sentral rules and regulations on outsourcing.	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.	Enabling Customer Compliance
40.	**ANNEX A**		
41.	Despite its many potential benefits, cloud computing also brings with it potential areas of concern, when compared with computing environments found in traditional data centers. Some of the more fundamental concerns include the following:		
42.	1. **Legal and Regulatory Compliance**		
43.	Important considerations for any BSFI before deploying a cloud computing model include clearly understanding the various types of laws and regulations that potentially impact cloud computing initiatives, particularly those involving confidentiality, visibility, data location, privacy and security controls and records management. The nature of cloud computing may increase the complexity of compliance with applicable laws and regulations because customer data may be stored or processed offshore. The BSFI's ability to assess compliance may be more complex and difficult in an environment where the Cloud Service Provider (CSP) processes and stores data overseas or comingles the BSFI's data with data from other customers that operate under diverse legal and regulatory jurisdictions. The BSFI should understand the applicability of local laws and regulations and ensure its contract with a CSP specify its obligations with respect to the BSFIs' responsibilities for compliance with relevant laws and regulations. CSP's processes should not compromise compliance with the following, among others: a. Law on Secrecy of Deposits (R.A. No. 1405); b. Foreign Currency Deposit System (R.A. No. 6426) c. Anti-Money Laundering Act, particularly on data/file retention; d. Electronic Commerce Act (R.A. No. 8792); e. Data Privacy Law; f. Cybercrime Prevention Act; g. General Banking Law (R.A. No. 8791); and h. Regulations concerning IT risk management, electronic banking, consumer protection, reporting of security incidents and other applicable Bangko Sentral issuances, rules and regulations.	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. Google 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.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
44.	Lastly, the CSP should grant Bangko Sentral access to its cloud infrastructure to determine compliance with applicable laws and regulations and assess soundness of risk management processes and controls in place.	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.	Regulator Information, Audit and Access
45.	**2. Governance and Risk Management**		
46.	The use of outsourced cloud services to achieve the BSFI's strategic plan does not diminish the responsibility of the Board of Directors and management to ensure that the outsourced activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations. The BSFI Management should consider overall business and strategic objectives prior to outsourcing the specific IT operations to the cloud computing platform. A Board-approved outsourcing policy and rationale for outsourcing to the cloud environment should be in place to ensure that the Board is fully apprised of all the risks identified.	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.	N/A

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
47.	Outsourcing to a CSP can be advantageous to a BSFI because of potential benefits such as cost reduction, flexibility, scalability, improved load balancing, and speed. However, assessing and managing risk in systems that use cloud services can be a formidable challenge due mainly to the unique attributes and risks associated with a cloud environment especially in areas of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality as well as legal issues such as regulatory compliance, auditing and data offshoring. Cloud computing may require more robust controls due to the nature of the service. When evaluating the feasibility of outsourcing to a CSP, it is important to look beyond potential benefits and to perform a thorough due diligence and risk assessment of elements specific to the service. Vendor management, information security, audits, legal and regulatory compliance, and business continuity planning are key elements of sound risk management and risk mitigation controls for cloud computing. As with other service provider offerings, cloud computing may not be appropriate for all BSFIs.	Risk management 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. Controls Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
48.	**3. Due Diligence**		
49.	The due diligence in selecting a qualified CSP is of paramount importance to ensure that it is capable of meeting the BSFI's requirements in terms of cost, quality of service, compliance with regulatory requirements and risk management. Competence, infrastructure, experience, track record, financial strength should all be factors to consider. When contemplating transferring critical organizational data to the cloud computing platform, it is critical to understand who and where all of the companies and individuals that may touch the BSFI's data. This includes not only the CSP, but all vendors or partners that are in the critical path of the CSP. Background checks on these companies are important to ensure that data are not being hosted by an organization that does not uphold confidentiality of information or that is engaging in malicious or fraudulent activity. Business resiliency and capability to address the BSFI's requirements for security and internal controls, audit, reporting and monitoring should also be carefully considered.	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. Competence • 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 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. Financial Information • You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct. • You can review Google's audited financial statements on Alphabet's Investor Relations page. • Locations • Information about the location of Google's facilities and where individual services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page.	N/A

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Subprocessors Google engages third party vendors to perform limited activities in connection with the services. Information about these vendors (including their locations) and the limited processing of customer data they are authorized to perform is available on our Google Workspace Subprocessor page.	
50.	**4. Vendor Management/Performance and Conformance**		
51.	It is always important to thoroughly review the potential CSP's contract terms, conditions and SLA. This is to ensure that the CSP can legally offer what it has verbally committed to and that the cloud risk from the CSP's service offerings is within the determined level of acceptable risk of the BSFI. The SLA should ensure adequate protection of information and have details on joint control frameworks. It should also define expectations regarding handling, usage, storage and availability of information, and specify each party's requirements for business continuity and disaster recovery. At a minimum, the SLA should cover the provisions required under existing rules and regulations on outsourcing.	SLAs The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Workspace Service Level Agreement page. Business Continuity and Disaster Recovery 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, 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	Services Business Continuity and Disaster Recovery
52.	A vendor management process should be in place that proactively monitors the performance of the CSP on an ongoing basis. This is also to guarantee availability and reliability of the services provided and ability to provide consistent quality of service to support normal and peak business requirements. If a BSFI is using its own data centre, it can mitigate and prepare for outages. However, if it is using a cloud computing service, it has to put all its trust in the cloud service provider delivering on its SLA. This requires that SLA has sufficient means to allow transparency into the way a CSP operates, including the provisioning of composite services which is a vital ingredient for effective oversight of system security and privacy by the BSFI.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). 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.	Ongoing Performance Monitoring Significant Developments

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
53.	Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Collection and analysis of available data about the state of the system should be done regularly and as often as needed by the BSFI to manage security and privacy risks, as appropriate for each level of the organization involved in decision making. Transition to public cloud services entails a transfer of responsibility to the CSP for securing portions of the system on which the BSFI's data and applications operate. To fulfill the obligations of continuous monitoring, the organization is dependent on the CSP, whose cooperation is essential, since critical aspects of the computing environment are under its complete control.	Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Refer to our security whitepaper for more information.	N/A
54.	Cloud services that allow CSP to further outsource or subcontract some of its services may also heighten concerns, including the scope of control over the subcontractor, the responsibilities involved (e.g., policy and licensing arrangements), and the remedies and recourse available should problems occur. A CSP that hosts applications or services of other parties may involve other domains of control, but through transparent authentication mechanisms, appear to the BSFI to be that of the CSP. Requiring advanced disclosure of subcontracting arrangements, and maintaining the terms of these arrangements throughout the agreement or until sufficient notification can be given of any anticipated changes, should be properly enforced.	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
55.	Additionally, the complexity of a cloud service can obscure recognition and analysis of incidents. The CSP's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Each layer in a cloud application stack, including the application, operating system, network, and database, generates event logs, as do other cloud components, such as load balancers and intrusion detection systems; many such event sources and the means of accessing them are under the control of the cloud provider. It is important that the CSP has a transparent response process and mechanisms to share information with the BSFI during and after the incident. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought. The geographic location of data is a related issue that can impede an investigation, and is a relevant subject for contract discussions. Revising the BSFI's incident response plan to address differences between the organizational computing environment and the cloud computing environment is also a prerequisite to transitioning applications and data to the cloud.	Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
56.	Lastly, to effectively monitor services including risk and risk mitigation associated with the use of a CSP, the BSFI and the CSP should agree in advance that former shall have accessibility to the CSP to audit and verify the existence and effectiveness of internal	Audit 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	Regulator Information, Audit and Access Customer Information, Audit and Access

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	and security controls specified in the SLA. The BSFI's audit policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing. It may also be necessary to augment the internal audit staff with additional training and personnel with sufficient expertise in evaluating shared environments and virtualized technologies. In addition, the parties may also agree on the right to audit clause via external party as a way to validate other control aspects that are not otherwise accessible or assessable by the BSFI's own audit staff. Ideally, the BSFI should have control over aspects of the means of visibility to accommodate its needs, such as the threshold for alerts and notifications, and the level of detail and schedule of reports.	regulated entities, supervisory authorities, and both their appointees. Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world. Third party audits reports Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ● ISO/IEC 27001:2013 (Information Security Management Systems) ● ISO/IEC 27017:2015 (Cloud Security) ● ISO/IEC 27018:2014 (Cloud Privacy) ● SOC 1 ● SOC 2 ● SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
57.	**5. Security and Privacy**		
58.	Security and privacy concerns continue to be a major issue within a cloud computing model. Given the obvious sensitivity of data and the regulated environment within which they operate, BSFIs utilizing cloud systems, need to have an assurance that any data exposed on the cloud is well protected. They may need to revise their information security policies, standards, and practices to incorporate the activities related to a CSP. They should also have an understanding of and detailed contracts with SLAs that provide the desired level of security to ensure that the CSP is applying appropriate controls. In certain situations, continuous monitoring of security infrastructure may be necessary for BSFIs to have a sufficient level of assurance that the CSP is maintaining effective controls.	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Security controls Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ● ISO/IEC 27001:2013 (Information Security Management Systems) ● ISO/IEC 27017:2015 (Cloud Security) ● ISO/IEC 27018:2014 (Cloud Privacy) ● SOC 1	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • **Encryption at rest.** Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. • **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources	

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google also publishes guidance on: • Security best practices • Security use cases	
59.	It is important that BSFIs maintain a comprehensive data inventory and a suitable data classification process, and that access to customer data is restricted appropriately through effective identity and access management. A multi-tenant cloud deployment, in which multiple clients share network resources, increases the need for data protection through encryption and additional controls such as virtualization mechanisms to address the risk of collating organizational data with that of other organizations and compromising confidential information through third-party access to sensitive information. Verifying the data handling procedures, adequacy and availability of backup data, and whether multiple service providers are sharing facilities are important considerations. If the BSFI is not sure that its data are satisfactorily protected and access to them is appropriately controlled, entering into a cloud service arrangement may not be suitable.	Data Segregation To keep data private and secure, Google logically isolates each customer's data from that of other customers. Data inventory and classification Google provides tools to help you manage your assets on our services. For example: • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Workspace resources. • Endpoint Management allows you to simplify endpoint management in your organization with Google Workspace. Enforce passcodes and wipe specific accounts without installing software on a user's Android and iOS device with agentless endpoint management. This feature is on by default. • 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. Encryption Encryption is central to Google's comprehensive security strategy. We provide certain encryption by default, with no additional action required from you. We also offer a continuum of encryption key management options to meet your needs. Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage, and rotation.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
60.	Storage of data in the cloud could increase the frequency and complexity of security incidents. Therefore, management processes of the BSFI should include appropriate notification procedures; effective monitoring of security-related threats, incidents and events on both BSFI's and CSP's networks; comprehensive incident response methodologies; and maintenance of appropriate forensic strategies for investigation and evidence collection.	Google will notify you of data incidents promptly and without undue delay. In addition, Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Refer to our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
61.	**6. Data Ownership and Data Location and Retrieval**		

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
62.	The BSFI's ownership rights over the data must be firmly established in the contract to enable a basis for trust and privacy of data. Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the CSP acquires no rights or licenses through the agreement, to use the BSFI's data for its own purposes; and that the CSP does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the CSP.	You retain all intellectual property rights in your data. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Intellectual Property Protection of Customer Data
63.	One of the most common challenges in a cloud computing environment is data location. Use of an in-house computing center allows the BSFI to structure its computing environment and to know in detail where data is stored and what safeguards are used to protect the data. In contrast, the dynamic nature of cloud computing may result in confusion as to where information actually resides (or is transitioning through) at a given point in time, since multiple physical locations may be involved in the process. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. One of the main compliance concerns is the possible transborder flows of data which may impinge upon varying laws and regulations of different jurisdictions.	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)
64.	To address the above constraints, the BSFI should pay attention to the CSP's ability to isolate and clearly identify its customer data and other information system assets for protection. Technical, physical and administrative safeguards, such as access controls, often apply. Likewise, such concerns can be alleviated if the CSP has some reliable means to ensure that an organization's data is stored and processed only within specific jurisdictions. Lastly, external audits and security certificates can mitigate the issues to some extent.	Data Segregation To keep data private and secure, Google logically isolates each customer's data from that of other customers. Data Location Selection Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum) Data Location (Service Specific Terms)

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Audits and Certifications Refer to Row 56 for information about the third party audit reports Google provides.	
65.	**7. Business Continuity Planning**		
66.	The BCP in a BSFI involves the recovery, resumption, and maintenance of the critical business functions, including outsourced activities. Due to the dynamic nature of the cloud environment, information may not immediately be located in the event of a disaster. Hence, it is critical to ensure the viability of the CSP's business continuity and disaster recovery plans to address broad-based disruptions to its capabilities and infrastructure. The plans must be well documented and tested. Specific responsibilities and procedures for availability, data backup, incident response and recovery should be clearly understood and stipulated. Recovery Time Objectives should also be clearly stated in the contract. It is critical for the BSFI to understand the existence and comprehensiveness of the CSP's capabilities as well as its level of maturity to ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner. Other BCP-related concerns which must be addressed by the BSFI and CSP include the following:	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. In particular, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired RTO and RPO for your applications.	Business Continuity and Disaster Recovery
67.	a. Prioritization arrangements in case of multiple/simultaneous disasters;	Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. Information about the location of Google's facilities and where services can be deployed is available on our Global Locations page. Refer to our "Architecting disaster recovery for cloud infrastructure outages" article for information about how Google Cloud is architected to minimize the frequency and scope of outages as well as an architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes.	N/A
68.	b. Retention of onsite and offsite back- up (Whether to maintain an up-to-date back- up copy of data at the BSFI's premises or stored with a second vendor that has no common points of failure with the CSP); and	Regulated entities can use Spinbackup as part of their backup routine. Refer to our solutions page for more information about how you can configure Spinbackup Google Workspace backup and restore your Google Workspace data. 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.	N/A

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
69.	c. Ability to synchronize documents and process data while the client-BSFI is offline.	Refer to Row 68.	
70.	**Appendix 103 - Documents required under the revised outsourcing framework for banks**		
71.	1. A comprehensive policy on outsourcing duly approved by the board of directors of the bank.	This is a customer consideration.	N/A
72.	2. Service level agreement of contract between the bank and the service provider, which shall, at a minimum, include all of the following:	The Google Cloud Financial Services Contract is the written contract between the parties.	N/A
73.	a. Complete description of the work to be performed or services to be provided;	The Google Workspace services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions
74.	b. Fee structure;	Refer to your Google Cloud Financial Services Contract. Prices and fee information are also publicly available on our Pricing page.	Payment Terms
75.	c. Provisions governing amendment and pre- termination of contract;	Refer to your Google Cloud Financial Services contract.	Amendments; Term and Termination
76.	d. Responsibility, fines, penalties and accountability of the service provider for errors, omissions and frauds;	Refer to your Google Cloud Financial Services Contract.	Liability
77.	e. Confidentiality clause covering all data and information; solidarity liability of service provider and bank for any violation of R.A. No. 1405, (the Bank Deposits Secrecy Law) actions that the bank may take against the service provider for breach of confidentiality or any form of disclosure of confidential information; and the applicable penalties;	Google makes robust confidentiality commitments in our contract. In particular, we commit to only use confidential information that you share with us in accordance with our contract and to protect that information from disclosure.	Confidentiality
78.	f. Segregation of the data of the bank from that of the service provider and its other clients;	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)
79.	g. Disaster recovery/business continuity contingency plans and procedures;	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.	Business Continuity and Disaster Recovery

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference		Google Cloud commentary	Google Cloud Financial Services Contract reference
80.	h.	Guarantee that the service provider will provide necessary levels of transition assistance if the bank decides to convert to other service providers or other arrangements;	Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.	Transition Assistance
81.	i.	Access to the financial information of the service provider;	You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and strategy. It also provides information about our organizational policies e.g. our Code of Conduct.	N/A
82.	j.	Access of internal and external auditors to information regarding the outsourced activities/ services which they need to fulfill their respective responsibilities;	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 and their appointees.	Customer Information, Audit and Access
83.	k.	Access of Bangko Sentral to the operations of the service provider in order to review the same in relation to the outsourced activities/ services;	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 supervisory authorities and their appointees.	Regulator Information, Audit and Access
84.	l.	Provision which requires the service provider to immediately take the necessary corrective measures to satisfy the findings and recommendations of Bangko Sentral examiners and those of the internal and/or external auditors of the bank and/or the service provider;	Google is committed to taking appropriate corrective or remedial actions if an audit on behalf of the regulated entity or the supervisory authority identifies unaddressed deviations in the Services operations and controls.	Customer Information, Audit and Access; Regulator Information, Audit and Access
85.	m.	Remedies for the bank in the event of change of ownership, assignment, attachment of assets, insolvency, or receivership of the service provider; and	Regulated entities can terminate our contract with advance notice for change of control and for Google's insolvency.	Term and Termination
86.	n.	Provision allowing the bank to cancel the contract by contractual notice of dismissal or extraordinary notice of cancellation if so required by the Bangko Sentral.	Regulated entities can elect to terminate our contract for convenience with advance notice if directed by a supervisory authority.	Term and Termination
87.	**Additional Requirements for IT outsourcing:**			
88.	o.	Provisions regarding on-line communication availability, transmission line security, and transaction authentication;	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. The SLAs contain Google's commitments regarding availability of the Services. The SLAs provide measurable performance standards and remedies for the services and are available on our Google Workspace Service Level Agreement page. In addition, Google provides tools to help you manage and scale your networks. Refer to our Google Cloud Networking Products page for more information. For example:	Services

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications. • Dedicated Interconnect is a high-performance option providing direct physical connections between your on-premises network and Google's network.	
89.	p. Responsibilities regarding hardware, software and infrastructure upgrades;	Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Our infrastructure security page describes the security of this 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 technical constraints and processes in place to support operational security.	N/A
90.	q. Mandatory notification by the service provider of all systems changes that will affect the bank;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also control changes to your use of the services. Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. We recognize that our approach to change management is important to your own change management processes. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services
91.	r. Details of all security procedures and standards;	The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page.	

Bangko Sentral ng Pilipinas - The BSP Manual of Operation for Banks

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
92.	s. Adequate insurance for fidelity and fire liability; and	Google will maintain insurance cover against a number of identified risks.	Insurance
93.	t. Ownership/maintenance of the computer hardware, software (program source code), user and system documentation, master and transaction data files.	You retain all intellectual property rights in your data. Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.	Intellectual Property
94.	3. Secretary's certificate on the minutes of meeting of the board of directors of the bank (or a local/regional management committee, in case of foreign banks), explicitly approving the activity to be outsourced, the determination of whether an outsourcing arrangement is considered material or non-material and the specific service provider with which the bank is entering into an outsourcing contract;	This is a customer consideration.	N/A
95.	4. Profile of the selected service provider; and	Information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Information about Google Cloud's leadership team is available on our Media Resources page. You can review Google's corporate and financial information on Alphabet's Investor Relations page. This provides information about our mission, business model and	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		strategy. It also provides information about our organizational policies e.g. our Code of Conduct.	
96.	5. A central record of all outsourcing arrangements which shall be periodically updated and shall form part of the corporate governance reviews undertaken by the bank.	This is a customer consideration.	N/A