BSP Manual of Regulations for Banks

Google Cloud Mapping

This document is designed to help financial institutions (“**regulated entity**”) supervised by the Central Bank of the Philippines (“**BSP**”) to consider the Manual of Regulations for Banks (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on Section 148 - Information Technology Risk Management, Section 149 - Business Continuity Management and Section 1002 - Consumer Protection Standards of the framework. For each section, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
1	**Part One - Organization, Management and Administration**		
2	**E. Risk Management**		
3	**148 Information Technology Risk Management**		
4	**a. IT Governance**		
5	**(1) Oversight and organization of IT functions** Accountability is a key concern of IT governance and this can be obtained with an organizational structure that has well-defined roles for the responsibility of information, business processes, applications, IT infrastructure, etc.		
6	The board of directors is ultimately responsible for understanding the IT risks confronted by a BSFI and ensuring that they are properly managed, whereas the senior management is accountable for designing and implementing the ITRMS approved by the board. For complex BSFIs, the board may delegate to an IT steering committee (ITSC) or its equivalent IT oversight function to cohesively monitor IT performance and institute appropriate actions to ensure achievement of desired results. The ITSC, at a minimum, should have as members a non-executive director who oversees the institution’s IT function, the head of IT group/department, and the highest rank officer who oversees the business user groups. The head of control groups should participate in ITSC meetings in an advisory capacity only.	This is a customer consideration.	N/A
7	A charter should be ratified by the board to clearly define the roles and responsibilities of the ITSC. Formal minutes of meeting should be maintained to document its discussions and decisions. The ITSC should regularly provide adequate information to the board regarding IT performance, status of major IT projects or other significant issues to enable the board to make well-informed decisions about the BSFIs’ IT operations.	This is a customer consideration.	N/A
8	BSFIs should develop an IT strategic plan that is aligned with the institution’s business strategy. This should be undertaken to manage and direct all IT resources in line with the business strategy and priorities. IT strategic plan should focus on long term goals covering three (3) to five (5) year horizon and should be sufficiently supplemented by tactical IT plans which specify concise objectives, action plans and tasks that are understood and accepted by both business and IT. The IT strategic plan should be formally documented, endorsed by the Board and communicated to all stakeholders. It should be reviewed and updated regularly for new risks or opportunities to maximize the value of IT to the institution.	This is a customer consideration.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
9	BSFIs should also create an organization of IT functions that will effectively deliver IT services to business units. For complex BSFIs, a full-time IT head or equivalent rank should be designated to take the lead in key IT initiatives and oversee the effectiveness of the IT organization. In addition to managing the delivery of day-to-day IT services, the IT head should also oversee the IT budget and maintain responsibility for performance management, IT acquisition oversight, professional development and training. The IT head should be a member of executive management with direct involvement in key decisions for the BSFI and usually reports directly to the president or chief executive officer.	This is a customer consideration.	N/A
10	A clear description of roles and responsibilities for individual IT functions should be documented and approved by the board. Proper segregation of duties within and among the various IT functions should be implemented to reduce the possibility for an individual to compromise a critical process. A mechanism should be in place to ensure that personnel are performing only the functions relevant to their respective jobs and positions. In the event that an institution finds it difficult to segregate certain IT control responsibilities, it should put in place adequate compensating controls (e.g. peer reviews) to mitigate the associated risks.	This is a customer consideration.	N/A
11	**(2) IT policies, procedures and standards.** IT controls, policies, and procedures are the foundation of IT governance structure. It helps articulate the rules and procedures for making IT decisions, and helps to set, attain, and monitor IT objectives.		
12	BSFIs should adopt and enforce IT-related policies and procedures that are well-defined and frequently communicated to establish and delineate duties and responsibilities of personnel for better coordination, effective and consistent performance of tasks, and quicker training of new employees. Management should ensure that policies, procedures, and systems are current and well-documented. The ITSC should review IT policies, procedures, and standards at least on an annual basis. Any updates and changes should be clearly documented and properly approved. IT policies and procedures should include at least the following areas: • IT Governance/ Management; • Development and Acquisition; • IT Operations; • Communication networks; • Information security; • Electronic Banking/Electronic Products and Services; and • IT Outsourcing/Vendor Management.	This is a customer consideration.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	For simple BSFIs, some of the above areas (i.e., development, electronic banking, etc.) may not be applicable, thus sound judgment should be employed to ensure that the BSFI's IT policies and procedures have adequately covered all applicable areas.		
13	**(3) IT audit.** Audit plays a key role in assisting the board in the discharge of its corporate governance responsibilities by performing an independent assessment of technology risk management process and IT controls.		N/A
14	Auditors provide an assurance that important control mechanisms are in place for detecting deficiencies and managing risks in the implementation of IT. They should be qualified to assess the specific risks that arise from specific uses of IT. BSFIs should establish effective audit programs that cover IT risk exposures throughout the organization, risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies and periodic reporting to the Board on the effectiveness of the institution's IT risk management, internal controls, and IT governance. Regardless of size and complexity, the IT audit program should cover the following: • Independence of the IT audit function and its reporting relationship to the Board or its Audit Committee; • Expertise and size of the audit staff relative to the IT environment; • Identification of the IT audit universe, risk assessment, scope, and frequency of IT audits; • Processes in place to ensure timely tracking and resolution of reported weaknesses; and • Documentation of IT audits, including work papers, audit reports, and follow-up. In case in-house IT audit expertise is not available, such as for a simple BSFI, the IT audit support may be performed by external specialists and auditors of other institutions consistent with existing Bangko Sentral rules and regulations on outsourcing.	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: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time.	Certifications and Audit Reports
15	**(4) Staff competence and training.** The rapid development in technology demands appropriate, skilled personnel to remain competent and meet the required level of expertise on an ongoing basis		
16	BSFIs should have an effective IT human resources management plan that meets the requirements for IT and the business lines it supports. Management should allocate sufficient resources to hire and train employees to ensure that they have the expertise necessary to perform their job and achieve organizational goals and objectives. Management needs to ensure that staffing levels are sufficient to handle present and expected work demands, and to cater reasonably for staff turnover. Appropriate succession and transition strategies for key officers and personnel should be in place to provide for a smooth transition in the event of turnover in vital IT management or operations functions.	This is a customer consideration.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
17	**(5) Management Information Systems (MIS)**		
18	The BSFIs' IT organization often provides an important support role for their MIS. Accurate and timely MIS reports are an essential component of prudent and reasonable business decisions. At the most senior levels, MIS provides the data and information to help the Board and management make strategic decisions. At other levels, MIS allows management to monitor the institution's activities and distribute information to other employees, customers, and members of management.	This is a customer consideration.	N/A
19	**(6) IT risk management function**		
20	Management of risk is a cornerstone of IT Governance. BSFIs should have a policy requiring the conduct of identification, measurement, monitoring and controlling of IT risks for each business function/service on a periodic basis. BSFIs should define and assign these critical roles to a risk management unit or to a group of persons from different units collectively performing the tasks defined for this function.	This is a customer consideration. Information about Google's approach to risk management is available in Google's certifications and audit reports. Refer to Row 14 for more information.	N/A
21	The function should have a formal technology risk acknowledgement and acceptance process by the owner of risk to help facilitate the process of reviewing, evaluating and approving any major incidents of non-compliance with IT control policies. The process can be supported by the following: • a description of risk being considered for acknowledgement by owner of risk and an assessment of the risk that is being accepted; • identification of mitigating controls; • formulation of a remedial plan to reduce risk; and • approval of risk acknowledgement from the owner of the risk and senior management ITRM processes should be integrated into the enterprise-wide risk management processes to allow BSFIs to make well-informed decisions involving business plans and strategies, risk responses, risk tolerance levels and capital management, among others	This is a customer consideration. Information about Google's approach to risk management is available in Google's certifications and audit reports. Refer to Row 14 for more information.	N/A
22	**b. Risk identification and assessment**		
23	BSFIs should maintain a risk assessment process that drives response selection and controls implementation. An effective IT assessment process begins with the identification of the current and prospective IT risk exposures arising from the institution's IT environment and related processes. The assessments should identify all information assets, any foreseeable internal and external threats to these assets, the likelihood of the threats, and the adequacy of existing controls to mitigate the identified risks. Management should continually compare its risk exposure to the value of its business activities to determine acceptable risk levels.	This is a customer consideration.	N/A
24	Once management understands the institution's IT environment and analyzes the risk, it should rank the risks and prioritize its response. The probability of occurrence and the magnitude of impact provide the foundation for reducing risk exposures or establishing	This is a customer consideration. Refer to Row 14 for more information.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	mitigating controls for safe, sound, and efficient IT operations appropriate to the complexity of the organization. Periodic risk assessment process should be done at the enterprise-wide level and an effective monitoring program for the risk mitigation activities should be manifested through mitigation or corrective action plans, assignment of responsibilities and accountability and management reporting.		
25	**c. IT controls implementation**		
26	Management should establish an adequate and effective system of internal controls based on the degree of exposure and the potential risk of loss arising from the use of IT. Controls for the IT environment generally should address the overall integrity of the environment and should include clear and measurable performance goals, the allocation of specific responsibilities for key project implementation, and independent mechanisms that will both measure risks and minimize excessive risk-taking.	This is a customer consideration. Refer to Row 14 for more information.	N/A
27	BSFI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy:		
28	**(1) Information security.**		
29	Information is a vital asset of a BSFI that must be adequately protected and managed to preserve its confidentiality, integrity and availability. Considering the crucial role information plays in supporting business goals and objectives, driving core operations and critical decision-making, information security is intrinsically linked to the overall safety and soundness of BSFIs. Thus, the BSFI needs to put in place a robust, resilient and enterprise wide framework for ISRM supported by effective information security governance and oversight mechanisms. Information security risk exposures must be managed to within acceptable levels through a dynamic interplay of people, policies and processes, and technologies and must be integrated with the enterprise-wide risk management system.	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. Information about Google's internal control environment and security history is available in Google's certifications and audit reports.You can review Google's current certifications and audit reports at any time. **Information security measures** The confidentiality and security of information when using a cloud service consists of two key elements: Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at:	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		- 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. 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 at: https://cloud.google.com/security/encryption-at-rest/default-encryption. - **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 at https://cloud.google.com/security/encryption-in-transit. (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	

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		- Security use cases Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of the effectiveness of our internal controls. To give you visibility of the effectiveness of our internal controls throughout our relationship, Google commits to maintain certifications / reports for 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) - PCI DSS - SOC 1 - SOC 2 - SOC 3 Use of your information Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Certifications and Audit Reports Protection of Customer Data
30	Management should adopt a holistic, integrated and cyclical approach to managing information security risks. An ISRM framework should be in place encompassing key elements and phases with effective governance mechanisms to oversee the entire process. The framework represents a continuing cycle that should evolve over time taking into account changes in the operating and business environment as well as the overall cyber-threat landscape.	This is a customer consideration. Refer to Row 29 for information on Google's information security measures.	N/A
31	**(2) Project management/development and acquisition and change management.**		
32	BSFIs should establish a framework for management of IT-related projects. The framework should clearly specify the appropriate project management methodology that will govern the process of developing, implementing and maintaining major IT systems. The methodology, on the other hand, should cover allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, checkpoints, key dependencies, quality assurance, risk assessment and approvals, among others. In the acquisition and/or development of IT solutions, BSFIs should ensure that business and regulatory requirements are satisfied.	This is a customer consideration.	N/A
33	**(3) IT Operations**		
34	IT has become an integral part of the day-to-day business operation, automating and providing support to nearly all of the business processes and functions within the institution. Therefore, the IT systems should be reliable, secure and available when needed which translates to high levels of service and dependency on IT to operate.	You can monitor Google's performance of the Services (including the SLAs) on a regular basis using the functionality of the Services. For example:	Services

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	One of the primary responsibilities of IT operations management is to ensure the institution's current and planned infrastructure is sufficient to accomplish its strategic plans. BSFI management should ensure that IT operates in a safe, sound, and efficient manner throughout the institution. Given that most IT systems are interconnected and interdependent, failure to adequately supervise any part of the IT environment can heighten potential risks for all elements of IT operations and the performance of the critical business lines of the BSFIs. Such a scenario necessitates the coordination of IT controls throughout the institution's operating environment.	- The Status Dashboard provides status information on the Services. - Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements. Refer to Row 29 for information on Google's information security measures.	
35	**(4) IT outsourcing/vendor management program.**		
36	IT outsourcing refers to any contractual agreement between a BSFI and a service provider or vendor for the latter to create, maintain, or reengineer the institution's IT architecture, systems and related processes on a continuing basis. A BSFI may outsource IT systems and processes except those functions expressly prohibited by existing regulations.	This is a customer consideration.	N/A
37	The decision to outsource should fit into the institution's overall strategic plan and corporate objectives and said arrangement should comply with the provisions of existing Bangko Sentral rules and regulations on outsourcing. Although the technology needed to support business objectives is often a critical factor in deciding to outsource, managing such relationships should be viewed as an enterprise-wide corporate management issue, rather than a mere IT issue.	This is a customer consideration.	N/A
38	While IT outsourcing transfers operational responsibility to the service provider, the BSFIs retain ultimate responsibility for the outsourced activity. Moreover, the risks associated with the outsourced activity may be realized in a different manner than if the functions were inside the institution resulting in the need for controls designed to monitor such risks.	This is a customer consideration.	N/A
39	BSFI management should implement an effective outsourcing oversight program that provides the framework for management to understand, monitor, measure, and control the risks associated with outsourcing.	This is a customer consideration. Google recognizes that using our Services should not impair a regulated entity's ability to oversee compliance with applicable laws and regulations as well as a regulated entity's internal policies. We will provide regulated entities with the assistance they need to review our Services.	Enabling Customer Compliance
40	IT services should have a comprehensive outsourcing risk management process which provides guidance on the following areas: 1) risk assessment; 2) selection of service providers; 3) contract review; and 4) monitoring of service providers.	Refer to row 39 for more information.	N/A

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
41	**(5) Electronic products and services**		
42	BSFIs should protect customers from fraudulent schemes done electronically. Otherwise, consumer confidence to use electronic channels as a safe and reliable method of making transactions will be eroded. To mitigate the impact of cyber fraud, BSFIs should adopt an aggressive security posture.	This is a customer consideration.	N/A
43	**d. Risk measurement and monitoring**		
44	BSFI Management should monitor IT risks and the effectiveness of established controls through periodic measurement of IT activities based on internally established standards and industry benchmarks to assess the effectiveness and efficiency of existing operations. Timely, accurate, and complete risk monitoring and assessment reports should be submitted to management to provide assurance that established controls are functioning effectively, resources are operating properly and used efficiently and IT operations are performing within established parameters. Any deviation noted in the process should be evaluated and management should initiate remedial action to address underlying causes.	This is a customer consideration.	N/A
45	The scope and frequency of these performance measurement activities will depend on the complexity of the BSFI's IT risk profile and should cover, among others, the following:		
46	(1) Performance vis-à-vis approved IT strategic plan. As part of both planning and monitoring mechanisms, BSFI management should periodically assess its uses of IT as part of overall business planning. Such an enterprise-wide and ongoing approach helps to ensure that all major IT projects are consistent with the BSFI's overall strategic goals. Periodic monitoring of IT performance against established plans shall confirm whether IT strategic plans remain in alignment with the business strategy and the IT performance supports the planned strategy.	You can monitor the 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. • Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • 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).	Ongoing Performance Monitoring
47	(2) Performance benchmarks/service levels. BSFIs should establish performance benchmarks or standards for IT functions and monitor them on a regular basis. Such monitoring can identify potential problem areas and provide assurance that IT functions are meeting the objectives. Areas to consider include system and network availability, data center availability, system reruns, out of balance conditions, response time, error rates, data entry volumes, special requests, and problem reports.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements. Refer to Row 46 for information on how you can monitor Google's performance of the Services.	Services

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	Management should properly define services and service level agreements (SLA) that must be monitored and measured in terms understandable to the business units. SLA with business units and IT departments should be established to provide a baseline to measure IT performance.		
48	(3) Quality assurance/quality control. BSFI should establish quality assurance (QA) and quality control (QC) procedures for all significant activities, both internal and external, to ensure that IT is delivering value to business in a cost effective manner and promotes continuous improvement through ongoing monitoring. QA activities ensure that product conforms to specification and is fit for use while QC procedures identify weaknesses in work products and to avoid the resource drain and expense of redoing a task. The personnel performing QA and QC reviews should be independent of the product/process being reviewed and use quantifiable indicators to ensure objective assessment of the effectiveness of IT activities in delivering IT capabilities and services.	Quality You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.	Ongoing Performance Monitoring
49	(4) Policy compliance. BSFIs should develop, implement, and monitor processes to measure IT compliance with their established policies and standards as well as regulatory requirements. In addition to the traditional reliance on internal and third party audit functions, BSFIs should perform self-assessments on a periodic basis to gauge performance which often lead to early identification of emerging or changing risks requiring policy changes and updates.	This is a customer consideration.	N/A
50	(5) External assessment program. Complex BSFIs may also seek regular assurance that IT assets are appropriately secured and that their IT security risk management framework is effective. This may be executed through a formal external assessment program that facilitates a systematic assessment of the IT security risk and control environment over time.	This is a customer consideration.	N/A
51	**Reporting and notification standards.**		
52	a. Reporting requirement. BSFIs are required to submit to the Bangko Sentral the following reports/information:		
53	(1) Periodic reports. BSFIs shall submit an Annual IT Profile, as listed in Appendix 7, electronically to the appropriate supervising department of the Bangko Sentral within twenty five (25) days from the end of reference year.	This is a customer consideration.	N/A
54	(2) Event-driven reports. BSFIs shall notify the Bangko Sentral upon discovery of any of the following:		
55	(a) Reportable Major Cyber-related Incidents. These cover all events which may seriously jeopardize the confidentiality, integrity or availability of critical information, data or systems of BSFIs, including their customers and other stakeholders. Reporting of such	Major cyber-related incidents Google will notify you of data incidents promptly and without undue delay. More	Data Incidents (Cloud Data Processing Addendum)

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	incidents to the Bangko Sentral should form part of the incident management plan of BSFIs.	information on Google's data incident response process is available in our Data incident response whitepaper.	
56	(b) Disruptions of financial services and operations. These include disruption of critical operations which lasts for more than two (2) hours due to internal and external threats, which may be natural, man-made or technical in origin. Such scenarios usually involve loss of personnel, technology, alternate sites, and service providers. Causes of such interruptions include, but are not limited to fire, earthquakes, flood, typhoon, long-term power outage, technical malfunctions, pandemics and other threats. Security events/attacks which are normally prevented by security systems/devices need not be reported to the Bangko Sentral, except if the same involves significant financial value and/or multitude of customer accounts beyond BSFI's reasonable threshold levels. For instance, an attempt to fraudulently transfer funds involving large sums of money requires immediate notification to the Bangko Sentral as this can be a signal of impending attacks to other BSFIs.	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 Incidents & the Google Cloud dashboard page	Significant events
57	**149 Business Continuity Management**		
58	**Business Continuity Management Framework.**		
59	BSFIs should adopt a cyclical, process-oriented BCM framework, which, at a minimum, should include five (5) phases, namely: BIA and risk assessment, strategy formulation, plan development, plan testing, and personnel training and plan maintenance. This framework represents a continuous cycle that should evolve over time based on changes in business and operating environment, audit recommendations, and test results. This framework should cover each business function and the technology that supports it. Other related policies, standards, and processes should also be integrated in the overall BCM framework.	This is a customer consideration.	N/A
60	**a. Business impact analysis and risk assessment.**		
61	A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their interdependencies through work-flow analyses, enterprise-wide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct a risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.	Information about how customers can use our Services in their own contingency planning is available in our Disaster Recovery Planning Guide. In particular, as part of your contingency planning, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments.	N/A
62	**b. Strategy formulation**		

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
63	Recovery and resumption strategies to achieve the agreed time-frame and deliver the minimum required services as identified in the BIA should be defined, approved, and tested. The minimum requirements for the provision of essential business and technology service levels during disruptions should be established by concerned business and support functions. (1) *Recovery strategy.* As business resumption relies primarily on the recovery of technology resources, adequate provisions should be in place to ensure systems availability and recoverability during disruptions as prescribed under *Appendix 77.* Recovery strategies should be able to meet the agreed requirements between business units and support functions for the provision of essential business and technology service levels. (2) *Continuity of operations/business resumption strategy.* The business continuity models adopted by the BSFI to handle prolonged disruptions should be based on the risk assessment of its business environment and the characteristics of its operations. The resumption strategies and resource requirements should be approved by the board as recommended by senior management or the relevant board committees to ensure alignment with corporate goals and business objectives.	This is a customer consideration. Refer to Row 65 for more information on Google's ability to provide disaster recovery and business continuity.	Services
64	**c. Plan development**		
65	Plans are an important, tangible evidence of the BSFI's business continuity initiatives. The objective of the plan is to provide detailed guidelines and procedures on response and management of a crisis, recovery of critical business services and functions and to ultimately resume normal operations. The plan should be formulated on an enterprise-wide basis, reviewed and approved by the board of directors and senior management at least annually and disseminated to all concerned employees. The plan should include provisions for both short-term and prolonged disruptions. A well-written plan should describe the various types of events or scenarios that could prompt BCP activation. It should include, at a minimum, the following components: (1) Escalation, declaration and notification procedures; (2) Responsibilities and procedures to be followed by each continuity or recovery teams and their members. The procedures should enable the BSFI to respond swiftly to a crisis (i.e., a crisis management plan) and to recover and resume the critical processes outlined in the plan within the stipulated time frame during disruptions;	Google recognizes the importance of business continuity and contingency planning. We do our own planning for our services. You can also use our services in your own business continuity and contingency planning. In addition, information about how customers can use our Services in their own business contingency planning is available in our Business Continuity Planning. In particular, as part of your contingency planning, you can choose to use Anthos build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments.	Business Continuity and Disaster Recovery

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	(3) A list of resources required to recover critical processes in the event of a major disruption. This would include, but not limited to: (a) key recovery personnel; (b) computer hardware and software; (c) communication systems; (d) office equipment; and (e) vital records and data; (4) Relevant information about the alternate and recovery sites; and (5) Procedures for restoring normal business operations. This should include the orderly entry of all business transactions and records during disruption into the relevant systems up to completion of all verification and reconciliation procedures.		
66	Communication is a critical aspect of a BCP. In this respect, the BSFI should include a communication plan for notifying all relevant internal and external stakeholders (e.g., employees, customers, vendors, regulators, counterparties, and key service providers, media and the public) following a disruption. The BSFI should maintain an up-to-date call tree and contact list of key personnel and service providers, including communication flow and channels for internal and external stakeholders. Clear and effective communication will facilitate escalation for appropriate management action and instruction to all concerned and help manage reputational risks. The BSFI should consider alternate methods of communication and preparation of predetermined messages tailored to a number of plausible disruption scenarios to ensure various stakeholders are timely, consistently, and effectively informed.	Refer to Row 65 for more information.	N/A
67	A crisis management plan should be included in the BCP to assist senior management in dealing with and containing an emergency and avoid spillover effects to the business. Senior management should identify potential crisis scenarios and develop corresponding crisis management procedures. This includes identifying a mix of individuals from various departments who are authorized to make instantaneous decisions during crisis situations. This team shall be responsible for the actual declaration of an event, activation of the plan, and internal and external communication process.	Refer to Row 65 for more information.	N/A
68	When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms to legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.	Refer to Row 65 for more information.	N/A
69	**d. Plan Testing**		
70	**(1) Types of testing methods**		

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
71	Plan testing is a vital element of the BCM. It ensures that the plan remains accurate, relevant, and operable. Tests should be conducted periodically, with the nature, scope, and frequency determined by the criticality of the applications, business processes, and support functions. In some cases, plan tests may be warranted due to changes in BSFI's business, responsibilities, systems, software, hardware, personnel, facilities, or the external environment. Testing methods can vary from simple to complex, each bearing its own characteristics, objectives, and benefits. Types of testing methods in order of increasing complexity include: (a) *Tabletop exercise/structured walk-through test* – the primary objective is to ensure that critical personnel from all areas are familiar with the plan and that it accurately reflects the BSFI's ability to recover from a disruption. (b) *Walk-through drill/simulation test* – similar to a tabletop exercise but with a more focused application. During this test, participants choose a specific scenario to which relevant plan provisions shall be applied. (c) *Communication/call tree test* – an exercise that validates the capability of crisis management teams to respond to specific events and the effectiveness of the call tree notification process in disseminating information to employees, vendors, and key clients. (d) *Alternate site test/exercise* – tests the capability of staff, systems, and facilities, located at alternate sites to effectively support production processing and workloads. (e) *Component test/exercise* – A testing activity designed to validate the continuity of individual systems, processes, or functions, in isolation. (f) *Functional drill/parallel test* – test to determine capability of alternate site and BSFI employees to support strategy as defined in the plan, which involves actual mobilization of personnel, establishing communications, and recovery processing. (g) *Enterprise-wide full-interruption/full-scale test* – the most comprehensive type of test encompassing the entire organization and requires activation of all the components of the plan at the same time to simulate a real-life emergency and processing data and transactions using backup media at the recovery site.	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. In addition, information about how customers can use our Services in their own business contingency planning is available on the Google Cloud Platform Disaster Recovery Planning Guide page.	Business Continuity and Disaster Recovery
72	**(2) Test policy/plan.**		
73	Testing should be viewed as a continuously evolving cycle. The BSFI should incorporate the results of BIA and risk assessment and work towards a testing strategy that increases in scope and complexity to address a variety of threat scenarios. Test scenarios should vary from isolated system failures to wide-scale disruptions and promote testing its primary and alternate facilities, as well as with key counterparties and third-party service providers.	Refer to Row 71 for more information.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	A testing policy should define roles and responsibilities for the implementation and evaluation of the testing program. Test plans with pre-determined goals and test criteria should be developed for each testing activity. It should clearly define the objectives of testing, identify the functions, systems, or processes to be tested and the criteria for assessing what constitutes a successful test. Formal testing documentation (i.e., test plans, test scenarios, test procedures, test results) should be prepared to ensure thoroughness and effectiveness of testing and properly maintained for audit and review purposes.		
74	**(3) Annual enterprise-wide business continuity testing.**		
75	The BSFI must conduct an enterprise-wide business continuity test at least annually, or more frequently depending on changes in the operating environment, to ensure its plan's relevance, effectiveness, and operational viability. The scope of testing should be comprehensive to cover the major components of the plan as well as coordination and interfaces among important parties.	Refer to Row 71 for more information.	N/A
76	**(4) Analysis and report of test results.**		
77	Plan tests, including successes, failures, and lessons learned, should be thoroughly analyzed to promote continuous BCM improvement. Exceptions noted should be documented and corrective actions should be closely monitored to ensure that they are implemented in a timely manner by concerned parties, including the board of directors and senior management, business line management, risk management, IT management, and other internal stakeholders.	This is a customer consideration.	N/A
78	**e. Personnel training and plan maintenance**		
79	**(1) *Training program.*** A business continuity training program should be provided to all concerned employees to promote awareness, familiarity, and understanding of their roles and responsibilities in the event of a disruption. The training program should be offered on a continuing basis for existing and new employees and should be updated to address changes to the plan.	Refer to row 65 for more information.	N/A
80	**(2) *Plan maintenance.*** Plans and results of BIA and risk assessment should be reviewed and updated on an ongoing basis (at least annually or when necessary) so that they remain consistent with the BSFI's current operations and business strategies.	Refer to row 65 for more information.	N/A
81	BCM-related documents (i.e., BCP, test program, policy guidelines, and program requirements) should be subject to change management process to ensure that these are updated with proper approval and documentation with respect to any significant changes in the business environment or as a result of audit findings.	Refer to row 65 for more information.	N/A
82	**Other policies, standards and processes.**		
83	**a. Pandemic planning.**		

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
84	(1) *Business impact analysis and risk assessment.* The BCM process should consider pandemics as early as the BIA and risk assessment phase. The BIA and risk assessment should be updated to incorporate complexities that may arise from pandemics, such as (a) increasing level of absenteeism based on a pandemic's severity; and (b) the need for another layer of contingency plans as regular disaster or emergency response methods are no longer feasible.	Refer to Row 65 for more information.	N/A
85	(2) *Strategy formulation.* To complement strategies for natural and technical disruptions, the following should be given due consideration when planning for pandemics: (a) *Trigger events* – Trigger events and strategies should be defined depending on the nature of a pandemic. Pandemic planning should have the flexibility to accommodate varying degrees of epidemic or outbreak as pandemics normally occur in waves or phases and of varying severity. (b) *Remote access capability* – In the event of a pandemic, enabling remote access may be one of the primary strategies available to a BSFI. To support a telecommuting strategy, the BSFI should ensure adequate capacity, bandwidth and authentication mechanisms in its technological infrastructure against expected network traffic or volume of transactions. (c) External parties – With pandemics not limited to the BSFI, establishing working relationships with external parties is an essential component. In addition to the communication plan for all relevant internal and external stakeholders, the BSFI should establish open relationships and communication channels with local public health and emergency response teams or other government authorities. The BSFI should inform concerned parties of any potential outbreaks and, at the same time, be aware of any developments in the expected scope and duration of a pandemic. (d) Employee awareness – As information becomes available from reputable sources or local agencies, the BSFI should ensure that steps to limit or reduce the risk of being affected by the pandemic are cascaded to its employees.	Refer to Row 65 for more information.	N/A
86	(3) *Plan development.* Pandemic plans should be commensurate with the nature, size and complexity of a BSFI's business activities and have sufficient flexibility to address the various scenarios that may arise. At a minimum, the pandemic plan should include: (a) Strategy that is scalable dependent on the extent and depth of the outbreak; (b) Preventive measures, including monitoring of current environment and hygiene tools available to employees; (c) Communication plan with internal and external stakeholders, including concerned local public health teams and government agencies; and	Refer to Row 65 for more information.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	(d) Tools, systems and procedures available to ensure continuity of its critical operations even with the unavailability of BSFI's staff for prolonged periods.		
87	(4) *Plan testing.* Test policy/plan should include strategies to assess capability to continue critical operations, systems and applications even in the event of a severe pandemic. When regular tests are unable to cover pandemic scenarios, separate pandemic plan tests should be carried out.	Refer to Row 65 for more information.	N/A
88	(5) *Personnel training and plan maintenance.* The plan should be updated as developments and information become available. As needed, employee training programs should cover pandemic risks, including the roles and responsibilities of each employee during pandemic situations.	Refer to Row 65 for more information.	N/A
89	**b. Cyber resilience.**		
90	Cyber-threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated. Recent cyber-attacks worldwide highlight, not only the degree of disruption to a BSFI's operations, but also the extent of reputational damage which could undermine public trust and confidence. As such, the BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities. Given the unique characteristics of cyber-threats and attacks, traditional back-up and recovery arrangements adopted by the BSFI may no longer be sufficient and even increase the damage to the BSFIs' network, operations and critical information assets. In worst case scenarios, back-up systems and alternate recovery sites are likewise affected rendering both sites inoperable. To ensure cyber resilience, the BSFI should take into consideration a wide-range of cyber-threat scenarios perpetrated from diverse threat sources (e.g., skilled hackers, insiders, state-sponsored groups) which seek to compromise the confidentiality, availability and integrity of its information assets and networks. Defensive strategies and innovative recovery arrangements should be explored that are commensurate with the BSFI's cyber-security risk exposures and aligned with its information security program in accordance with Appendix 75.	Refer to Row 29 for information on Google's information security measures.	N/A
91	**c. Information Security**		
92	Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. Security during disasters and disruptions is an important consideration to manage risks arising from the change in working environment. The relevant guidelines/standards on information security that may be considered in strategy formulation and/or in choosing alternate sites are in Appendix 75.	Refer to Row 29 for information on Google's information security measures.	N/A
93	**d. Interdependencies**		
94	An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from	Refer to Row 65 for more information.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	interdependencies. The BSFI may have a very complex operating and recovery environment wherein interdependencies need to be duly considered, such as telecommunications, third party service providers, and recovery sites. Given the critical resources and services that are being shared with the BSFI or other entities, additional mitigating controls and recovery strategies need to be integrated in the plan.		
95	**e. Liquid risk management**		
96	Sound liquidity risk management practices enable a BSFI to maintain availability of funds even in times of financial stress or adverse changes in market conditions. In the event of a business disruption, sound liquidity risk management practices should similarly apply. The BSFI should ensure it has sufficient liquidity to support its recovery strategies and continue supporting the delivery of basic banking services to the clients pending full business resumption. Guidelines on liquidity risk management are in *Appendix 71*.	Refer to Row 65 for more information.	N/A
97	**f. Project management**		
98	Senior management should ensure that availability and business continuity requirements are considered at the planning and development stages of new business products and services and other critical technology processes, such as systems development and acquisition, and change management.	This is a customer consideration.	N/A
99	**g. Event/problem management**		
100	Operations personnel should be properly trained to recognize events that could trigger implementation of the plan. Although an event may not initially activate the plan, it may become necessary as conditions and circumstances change. Management should train and test BSFI personnel to implement and perform appropriate business continuity procedures within the timeframes of the plan.	This is a customer consideration. All relevant data center employees at Google receive regular training on contingency planning and executing recovery procedures.	Technical Support
101	**h. Outsourcing**		
102	When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations. Detailed guidelines/standards on business continuity considerations for outsourcing arrangements are in *Appendix 77*.	Refer to Row 65 for more information on Google's ability to provide disaster recovery and business continuity.	N/A
103	**i. Insurance**		
	Insurance is an option available to a BSFI for recovery of losses that cannot be completely prevented and the expenses related to recovering from a disruption. The BSFI should regularly review the adequacy and coverage of its insurance policies in reducing any foreseeable risks caused by disruptive events, such as loss of offices, critical facilities and equipment, and casualty. Insurance policies may also need to address the BSFI's legal responsibilities for failing to deliver services to its customers and counterparties. To facilitate the claims process, the BSFI should create and retain a	This is a customer consideration.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	comprehensive hardware and software inventory list in a secure off-site location and detailed expenses should be documented to support insurance claims.		
104	***Supervisory enforcement actions.*** BSFIs should make available all policies and procedures and other documents/information related to the foregoing during on-site examination as well as provide copies thereof to the regulator when a written request is made to determine compliance.	This is a customer consideration.	N/A
105	**Part Ten: BANGKO SENTRAL REGULATIONS ON FINANCIAL CONSUMER PROTECTION**		
106	**Section 1002: Consumer Protection Standards**		
107	**Protection of client information.**		
108	The BSFI demonstrates the ability to protect client information if it is able to:		
109	**a. Confidentiality and security of client information**		
110	(1) Have a written privacy policy to safeguard its customers' personal information. This policy should govern the gathering, processing, use, distribution, storage, and eventual disposal of client information. The BSFI should ensure that privacy policies and sanctions for violations are implemented and strictly enforced.	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. Confidentiality and Security Refer to row 29 for more information.	Data Security; Security Compliance by Google Staff (Cloud Data Processing Addendum)
111	(2) Ensure that privacy policies are regularly communicated throughout the organization. Opportunities include employees' initial training sessions, regular organization-wide training programs, employee handbooks, posters and posted signs, company intranet and internet websites, and brochures available to clients.	Refer to row 110 for more information.	N/A
112	(3) Have appropriate systems in place to protect the confidentiality and security of the personal data of its customers against any threat or hazard to the security or integrity of the information and against unauthorized access. This includes a written information security plan that describes its program to protect customer personal information. The plan must be appropriate to its size and complexity, nature and scope of its activities, and the sensitivity of customer information it handles. As part of its plan, the BSFI must: (a) Designate an employee accountable to coordinate its Information Security Program. (b) Identify and assess the risks to customer information in each relevant area of the BSFI operation, and evaluate the effectiveness of the current safeguards for controlling these risks. (c) Design and implement a safeguards program, and regularly monitor and test it. (d) Select service providers that can maintain appropriate safeguards. (e) Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.	Refer to row 110 for more information.	N/A

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
113	(4) Have appropriate policies and practices for employee management and training to assess and address the risks to customer information. These include:		
114	(a) Checking references and doing background checks before hiring employees who will have access to customer information.	Background checks Google conducts background checks on our employees where legally permissible to provide a safe environment for our customers and employees.	N/A
115	(b) Asking new employees to sign an agreement to follow BSFI confidentiality and security standards for handling customer information.	This is a customer consideration.	N/A
116	(c) Limiting access to customer information to employees who have a business reason to see it.	Refer to row 110 for more information.	N/A
117	(d) Controlling access to sensitive information by requiring employees to use “strong” passwords that must be changed on a regular basis.	Refer to row 29 for more information around how Google controls access to sensitive information.	N/A
118	(e) Using automatic time-out or log-off controls to lock employee computers after a period of inactivity.	Refer to row 29 for more information.	N/A
119	(f) Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information. These may include locking rooms and file cabinets where records are kept; ensuring that employee passwords are not posted in work areas; encrypting sensitive customer information when transmitted electronically via public networks; referring calls or other requests for customer information to designated individuals who have been trained in how BSFI safeguards personal data; and reporting suspicious attempts to obtain customer information to designated personnel.	Refer to row 29 for more information.	N/A
120	(g) Regularly reminding all employees of company policy to keep customer information secure and confidential.	Refer to row 29 for more information.	N/A
121	(h) Imposing strong disciplinary measures for security policy violations.	Refer to row 29 for more information.	N/A
123	(i) Preventing terminated employees from accessing customer information by immediately deactivating their passwords and usernames and taking other measures.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security and access.	Data Security; Security Measures (Cloud Data Processing Addendum)
124	(5) Have a strong IT System in place to protect the confidentiality, security, accuracy, and integrity of customer's personal information. This includes network and software design, and information processing, storage, transmission, retrieval, and disposal. Maintaining security throughout the life- cycle of customer information, from data entry to disposal, includes:		

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
125	(a) Knowing where sensitive customer information is stored and storing it securely. Make sure only authorized employees have access.	Locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. • Information about the location of Google's sub processors' facilities is available on our Google Cloud subprocessors page. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendums)
126	(b) Taking steps to ensure the secure transmission of customer information.	Refer to Row 29 for information about the security of the services, including information on encryption of data at rest and in transit.	N/A
127	(c) Disposing customer information in a secure way.	Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by the appropriate operations manager before release. For more information, please see: Data deletion on Google Cloud Platform | Documentation. See also the Decommissioned disks and disk erase policy in the Cloud Data Processing Addendum.	Appendix 2: Security measures (Cloud Data Processing Addendum)
128	(d) Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access.	Refer to row 14 for more information around Google's access controls.	N/A
129	(e) Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.	Refer to row 14 for more information around frameworks and procedures that Google maintains as part of third party audits.	N/A
130	(f) Having a security breach response plan in the event the BSFI experiences a data breach.	Security breaches 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)
131	**b. Sharing of customer information**		
132	(1) Inform its customers in writing and explain clearly to customers as to how it will use and share the customer's personal information.	Refer to row 130 for more information.	N/A

BSP Manual of Regulations for Banks

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
133	(2) Obtain the customers' written consent, unless in situations allowed as an exception by law or BSP-issued regulations on confidentiality of customer's information, before sharing customers' personal information with third parties such as credit bureau, collection agencies, marketing and promotional partners, and other relevant extern(4) Appropriate penalties should be imposed by the BSFI to erring employees for exposing or revealing client data to third parties without prior written consent from client.al parties.	Refer to row 130 for more information.	N/A
134	(3) Provide access to customers to the information shared and should allow customers to challenge the accuracy and completeness of the information and have these amended as appropriate.	Refer to row 130 for more information.	N/A
135	(4) Appropriate penalties should be imposed by the BSFI to erring employees for exposing or revealing client data to third parties without prior written consent from the client.	This is a customer consideration.	N/A
136	**Fair Treatment: e. Institutional culture of fair and responsible treatment of clients**		
137	(10) Perform appropriate due diligence before selecting the authorized agents/ outsourced parties (such as taking into account the agents' integrity, professionalism, financial soundness, operational capability and capacity, and compatibility with the FI's corporate culture) and implement controls to monitor the agents' performance on a continuous basis. The BSFI retains ultimate accountability for outsourced activities.	This is a customer consideration.	N/A