



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1137
Series of 2022

Subject : **Amendments to Regulations on Outsourcing and IT Risk Management**

The Monetary Board, in its Resolution No. 190 dated 10 February 2022, approved the amendments to Sections 112, Appendices 78 and 103 of the Manual of Regulations for Banks (MORB) and Sections 111-Q/113-S/112-P/102-N/112-T and Appendices Q-36/Q-65 of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

Section 1. Section 112 of the MORB on outsourcing shall be amended, as follows:

"112 MANAGEMENT CONTRACTS AND OUTSOURCING

xxx

***Outsourcing.* Xxx**

Definition. Xxx. Banks shall assess whether an outsourcing arrangement is material or non-material to the business. An outsourcing arrangement shall be considered material if a business disruption of an outsourced activity, service delivery failure and/or data/security breach will result in significant impact to bank's operations, financial condition, reputation, customers, and compliance with laws, rules and regulations.

Prohibition against outsourcing of inherent banking functions. No bank shall outsource inherent banking functions such as:

- a. Taking of deposits from the public;
- b. Granting of loans and extension of other credit exposures;
- c. Managing of risk exposures; and
- d. General management.

Authority to outsource. For material outsourcing arrangement, only banks with a SAFr composite rating¹ of at least “3” shall be allowed to outsource designated activities without prior Bangko Sentral approval, subject to notification requirements provided in Appendix 149 – Section B. Banks with SAFr rating of below “3” must secure approval from the appropriate supervising department² of the Bangko Sentral prior to the implementation of material outsourcing arrangements (see Appendix 149 – Section C for the list of requirements), which covers any of the following:

- a. New material outsourcing arrangements;
- b. Changes in existing material outsourcing arrangements that have significant impact in the delivery of outsourcing services, business operations, reputation and profitability; and
- c. Changes in existing outsourcing arrangements resulting in the reclassification of the arrangements as material such as, but not limited to those affecting the nature, scope, and complexity of systems and processes.

Governance and managing of outsourcing risks. xxx

- a. Conduct materiality assessment (see Annex “A”) of the outsourcing activity, which shall consider the following factors:

(1) Level of importance xxx

xxx

(5) Exposure to risk of confidentiality xxx

Periodic assessments shall be conducted to ensure that outsourcing risks, both on a contract-specific level and on an institution-wide level, are managed vis-à-vis the impact to the overall operations.

In cases when the risk management system xxx

- b. Establish policies and criteria xxx

xxx

¹ In lieu of the SAFr composite rating, the CAMELS composite rating of at least “3” shall be used. If neither a SAFr nor CAMELS rating is available, other BSP rating may be used as basis provided that the overall assessment of the BSFI satisfies the descriptive criteria of SAFr composite rating “3”, as follows: *BSFI is stable. Risks are adequately managed across the organization. Supervisory concerns are within the ability of the board and management to address. The BSFI's buffers will enable it to withstand most adverse events.*

² Technology outsourcing applications/notifications shall be submitted to the Technology Risk and Innovation Supervision Department (TRISD). Meanwhile, non-technology outsourcing applications/notifications shall be submitted to the respective Financial Supervision Department (FSD).

- f. Ensure the portability of the outsourced service (e.g., degree of difficulty, cost, and time in switching to an alternative service provider or to bring the activity in-house) and the impact to business continuity and recovery and resolution plans of the financial institution.

XXX

Other types of outsourcing arrangements. The guidelines and requirements of outsourcing to third-party service providers shall be observed when a bank (i) acts as the service provider, (ii) participates in intra-group outsourcing, or (iii) engages in offshore outsourcing.

a. Bank as a service provider. The bank may enter into an outsourcing agreement outside its business group, provided that the bank delivering the outsourced service shall adhere to the guidelines on outsourcing, as well as relevant laws and pertinent Bangko Sentral rules and regulations. It may also render services to its own depositors on account of the bank acting as the depository institution.

The service provider and service recipient should establish a clear understanding on rights and responsibilities on management of risks attendant to the outsourced activity, compliance with relevant laws, rules and regulations, and establishment of complaints handling and resolution process.

b. Intra-group outsourcing. Banks may enter into an intra-group outsourcing agreement without prior Bangko Sentral approval, in case: (i) the services rendered are performed in the ordinary course of business; (ii) the service provider is likewise a regulated financial institution; and (iii) the service is rendered to subsidiaries, affiliates and companies related to the service provider through common ownership.

The intra-group service provider may enter into a subcontracting agreement provided that said arrangement is regulated and authorized, as applicable, by the intra-group service provider's relevant regulatory authority.

The bank should ensure that the service provider has a sound financial condition and has the necessary competency to provide such service.

c. Offshore outsourcing. Offshore outsourcing of bank's domestic operations is permitted only when: (i) the service agreement defines counterparties' right and responsibilities on confidentiality and data privacy; and (ii) the service provider operates in jurisdictions with existing confidentiality and/or data privacy laws that are not in conflict with existing Philippine laws and relevant regulations.

When the service provider is located in other countries, the bank should take into account and closely monitor, on continuing basis, government policies and other conditions in countries where the service provider is based during the risk assessment process. The bank shall also develop appropriate contingency and exit strategies. Meanwhile, a domestic subsidiary of a foreign bank may enter into a material offshore intra-group outsourcing agreement without prior Bangko Sentral approval, provided that the outsourcing service is either engaged or provided by its parent bank, central service operations center, or designated entity within the group, which are duly regulated in their respective home jurisdictions.

The bank shall have the primary responsibility to ascertain the adequacy of design and effectiveness of service provider's security control mechanisms through audit procedures conducted by third party auditors or bank's internal audit function. In the event that results from alternative audit mechanism and third-party validation do not satisfy the objectives and requirements of the outsourcing regulations, the Bangko Sentral shall obtain from the bank relevant information in relation to the outsourced operations. If reasonable means to conduct offsite procedures have been exhausted, the Bangko Sentral shall be given access to the service provider and those relating to the outsourced domestic operations of the bank. Such access may be fulfilled through coordination with host authorities, if necessary. The domestic subsidiary of a foreign bank shall be principally liable in cases where the clients are prejudiced due to errors, omissions and frauds of the service provider located offshore.

The Bangko Sentral may require the bank to terminate xxx.

Section 2. The amendments to Appendices 103 and Q-36 of the MORB and MORNBFi, respectively, are attached as Annex "B" of this Circular.

Section 3. Appendix 78 of the MORB (IT Risk Management Standards and Guidelines, Area: IT Outsourcing/Vendor Management) on emerging outsourcing models shall be amended as follows:

xxx

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. For arrangements involving data transfer and handling, BSFI's should identify potential risks arising from physical and logical access of Technology Service Provider (TSP) employees, subcontractors, and other parties. As such, background checks on these

logical access of Technology Service Provider (TSP) employees, subcontractors, and other parties. As such, background checks on these companies are important to ensure that data are not being hosted by an organization that has a history or track record of not upholding confidentiality of information or that is engaging in malicious or fraudulent activity. Business resilience and technical capability of the TSP in providing security and controls, audit and compliance, monitoring, and reporting requirements of the BSFI should also be carefully considered. Contract negotiation should xxx

xxx

xxx

3.6 Security and Privacy. With growing concerns on data privacy and data security, BSFIs shall ensure that all confidential and sensitive data and information exposed to the TSP environment are well-managed and protected. BSFIs shall ensure that all data being handled, processed, and/or stored thru an outsourcing arrangement are included in its data inventory and data classification process. BSFIs shall likewise ensure that TSPs follow appropriate data handling procedures and employ robust access control mechanisms.

Moreover, BSFIs shall see to it that the TSP conducts periodic monitoring and reporting of security-related threats, incidents, and events on its networks/systems. The TSP should also have proactive incident response and problem management process in place, equipped with digital forensic tools and capabilities.

In order to assess the TSP's ability to enforce appropriate technical, physical, and administrative safeguards (i.e., access controls, data segregation, etc.) across its organization, BSFIs may refer to independent assessments (e.g., external audit, security certificates, among others) which provide attestation on the effectiveness of the TSP's control environment and security mechanisms.

3.7 Data Ownership and Data Location and Retrieval. One of the most common areas of concern in technology outsourcing is data transit, storage, and retrieval particularly in view of the multi-region cloud deployment setup. Such arrangement heightens challenges in assessing the design and control effectiveness of systems and processes across multiple physical locations. Moreover, laws, rules, regulations, and other compliance requirements may widely vary across jurisdictions where data is being transmitted, processed, and/or stored.

To address this, BSFIs must obtain a sound understanding of the TSP's physical and logical controls over its information assets. BSFIs should be able to identify where the data is being processed and/or stored and assess

whether the corresponding jurisdictions uphold data sovereignty laws. In any case, BSFIs should ensure that ownership rights over its data must be clearly defined in the contract to establish the proper level of data access and control. At a minimum, the contract should contain the following provisions: i) the BSFI retains exclusive ownership over all of its data; ii) the TSP acquires no rights whatsoever to use the BSFI's data for its own purpose or for any purpose other than what is required based on the scope of service; and iii) the TSP does not have the right to prevent the duly authorized access of BSFI to its own data. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the TSP.

3.8 Business Continuity Planning Consideration. The BSFI should integrate the TSP's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that the TSP tests its plan annually and notify the institution of any resulting modifications. BSFIs shall likewise establish contingency plans in case the TSP becomes unavailable or inaccessible. Appropriate contingency and resumption strategies should be formulated to consider both short-term and prolonged unavailability/inaccessibility of the TSP.

3.9 Compliance with Bangko Sentral Regulations. xxx

Section 4. Section 4 of Appendix 78 of the MORB (IT Risk Management Standards and Guidelines, Area: IT Outsourcing/Vendor Management) on emerging outsourcing models and Annex A of Appendix 78 of the MORB shall be deleted.

Section 5. Section 112-T of the MORNBFIs is hereby amended to read, as follows:

"Section 112-T *Guidelines on Outsourcing.* The rules on outsourcing of services as shown under Sec. 112 of the MORB and *Appendix Q-36*, in so far as applicable, shall apply to TCs.

Section 6. Effectivity. This Circular shall take effect fifteen (15) calendar days following its publication either in the Official Gazette or in a newspaper of general circulation.

FOR THE MONETARY BOARD:


BENJAMIN E. DIOKNO
Governor

18 February 2022

OUTSOURCING MATERIALITY ASSESSMENT
Compliance with Section 112 and Appendix 78 IT Outsourcing/Vendor Management
of the Manual of Regulations for Banks

FACTORS IN EVALUATING THE IMPACT OF THE SERVICE PROVIDER TO THE OVERALL OPERATIONS OF THE BANK	BSFI ASSESSMENT
(1) Level of importance to the bank of the activity to be outsourced and potential impact on bank's operations, financial condition, reputation, and ability to achieve its objectives, strategies and plans, should the service provider fail to perform the services;	
(2) Outsourcing costs in proportion to total operating expenses and compared with costs of developing own infrastructure and expertise;	
(3) Aggregate exposure to a particular service provider, in cases when the bank outsources various functions to the same service provider;	
(4) Ability to maintain appropriate controls and meet regulatory requirements, in cases of operational constraints of the service provider; and	
(5) Exposure to risk of confidentiality, integrity and availability of customer and bank data.	
OVERALL MATERIALITY ASSESSMENT (Material/Non-Material):	

**DOCUMENTS REQUIRED UNDER THE REVISED OUTSOURCING
FRAMEWORK FOR BSFIs**
**[Appendix to Sections 112, 111-Q, 701-Q (Outsourcing of internet and
mobile electronic services), 113-S, 162-P and 102-N]**

Section A. For all outsourcing arrangements

An outsourcing register covering all outsourcing arrangements of the BSFI shall be maintained and made available upon request of the Bangko Sentral. At a minimum, the following information should be included:

1. Outsourced Service¹
2. Description of Outsourced Service
3. Materiality (Material or Non-Material)
4. If material, date of BSP approval (if applicable)
5. Outsourcing arrangement
 - 5.1. Technology or Non-Technology
 - 5.2. Intragroup or Third-Party
6. Name of Service Provider
7. Business Address of Service Provider
8. Has the BSFI identified an Alternate Service Provider? (yes/no)
 - 8.1. If yes, name of the Alternate Service Provider
9. If cloud outsourcing, indicate the following:
 - 9.1. Cloud service model (IaaS, PaaS, SaaS, etc.)
 - 9.2. Cloud deployment model (Private, Public, Community, Hybrid)
10. Outsourcing agreement
 - 10.1. Start date
 - 10.2. Last renewal date (if applicable)
 - 10.3. End date
11. Does it involve deposit/customer information? (yes/no)
 - 11.1. If deposit/customer information is involved, location where outsourcing services are performed
12. Business Continuity Plan of the Service Provider
 - 12.1. Date last tested
13. Due Diligence/Periodic Service Performance Assessment
 - 13.1. Date last conducted
 - 13.2. Conducted by
14. Independent and/or third-party audit/review
 - 14.1. Date last conducted
 - 14.2. Conducted by

¹ Each service indicated in the master service agreement should be listed in a separate row.

Section B. For material outsourcing that DO NOT REQUIRE prior Bangko Sentral approval

Submit to the appropriate supervising department of the Bangko Sentral at least 30 banking days prior to the implementation of new or changes in material outsourcing arrangement, the following requirements:

1. Notification letter signed by the president or officer of equivalent rank, indicating that the BSFI will engage in material outsourcing arrangement/s, including the description of the outsourcing arrangement/s;
2. Corporate secretary's certificate on the approval of the board of directors of the BSFI (or a local/regional management committee, in case of foreign banks), of the outsourcing activity, including the determination of whether an outsourcing arrangement is considered material or non-material and the specific service provider with which the BSFI is entering into an outsourcing contract; and
3. Certification signed by the president or officer of equivalent rank and the Chief Compliance Officer (CCO), certifying that the BSFI has complied with all the prudential criteria under Section 111 of the MORB or Section 111-Q of the MORNBF on licensing, whichever is applicable, including the conduct of risk assessment of the outsourcing arrangement indicating the results thereof, as well as the contractual provisions pursuant to Appendix 78 and established sound risk management system on the following areas:
 - a. Legal and Regulatory Compliance;
 - b. Governance and Risk Management;
 - c. Due Diligence;
 - d. Vendor Management/Performance and Conformance;
 - e. Security and Privacy;
 - f. Data Ownership and Data Location and Retrieval; and
 - g. Business Continuity Planning

Within the 30-day period, the Bangko Sentral reserves the right to require additional documents from the BSFI relative to the material outsourcing arrangement and correspondingly, issue a notice of no objection. In the absence of such notice after the lapse of the 30-day period, BSFIs may proceed with the implementation of the material outsourcing arrangement.

Section C. For material outsourcing that REQUIRE prior Bangko Sentral approval

Submit to the appropriate supervising department of the Bangko Sentral at least 35 banking days prior to the implementation of new or changes in material outsourcing arrangement, the following requirements:

1. Application letter signed by the president or officer of equivalent rank signifying the BSFI's intent/plans to engage in material outsourcing arrangement/s, including the description of the outsourcing arrangement/s;
2. A comprehensive policy on outsourcing, duly approved by the board of directors of the BSFI.
3. Proposed master service agreement or contract between the BSFI and the service provider, which shall, at a minimum, include all of the following:
 - a. Complete description of the work to be performed or services to be provided;
 - b. Fee structure;
 - c. Provisions governing amendment and pre- termination of contract;
 - d. Responsibility, fines, penalties, and accountability of the service provider for errors, omissions, and frauds;
 - 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;
 - f. Segregation of the data of the BSFI from that of the service provider and its other clients;
 - g. Disaster recovery/business continuity contingency plans and procedures;
 - h. Guarantee that the service provider will provide necessary levels of transition assistance if the BSFI decides to convert to other service providers or other arrangements;
 - i. Access to the financial information of the service provider;

- j. Access of internal and external auditors to information regarding the outsourced activities/ services in line with the fulfillment of their respective responsibilities;
- 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 in the event that results of alternative audit mechanisms (i.e., independent review or validation, third-party attestation, etc.) do not satisfy the requirements and supervisory objectives of the Bangko Sentral;
- l. Provision which requires the service provider to promptly 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 BSFI and/or the service provider;
- m. Remedies for the BSFI in the event of change of ownership, assignment, attachment of assets, insolvency, or receivership of the service provider; and
- n. Provision allowing the BSFI to cancel the contract by contractual notice of dismissal or extraordinary notice of cancellation if so required by the Bangko Sentral due to non-compliance with regulatory requirements.

Additional Requirements for IT outsourcing:

- o. Provisions regarding on-line communication availability, transmission line security, and transaction authentication;
- p. Responsibilities regarding hardware, software, and infrastructure upgrades;
- q. Mandatory notification by the service provider of all systems changes that will affect the bank;
- r. Details of all security procedures and standards;
- s. Adequate general insurance coverage (e.g., fidelity and fire liability), if applicable; and
- t. Ownership/maintenance of the computer hardware, software (program source code), user and system documentation, master and transaction data files.

4. Corporate secretary's certificate on the minutes of meeting of the board of directors of the BSFI (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 BSFI is entering into an outsourcing contract;
5. Profile of the selected service provider;
6. If outsourcing an IT service involving cloud service provider, a Service Organization Control (SOC) 2 Type 2 or any equivalent Third Party/Independent Report;
7. Certification signed by the president or officer of equivalent rank and the Chief Compliance Officer (CCO), certifying the results of the risk assessment conducted on the outsourcing arrangement with the service provider;
8. Certification signed by the president or officer of equivalent rank and the Chief Compliance Officer (CCO), certifying that the BSFI has assessed the outsourcing arrangement as "material outsourcing" based on the factors enumerated in Section 112 of the MORB on governance and management of outsourcing risks; and
9. Accomplished IT Outsourcing Questionnaires and details of compliance with the requirements on IT Outsourcing/Vendor Management of Section 148 and Appendix 78 of the MORB/Section 147-Q/145-S/142-P/126-N/Appendix Q-65 of the MORNBF, as shown in Appendices 149-1 and 149-2. Ensure that supporting documents are attached and specific references thereto are clearly indicated.

IT OUTSOURCING QUESTIONNAIRE FOR BSFI
Compliance with Section 112 and Appendix 78 of the Manual of Regulations for Banks (MORB) and Appendix Q-65 of
the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI)
on IT Outsourcing/Vendor Management

Note: This self-assessment should be maintained by high-level officers who have direct understanding of the institution's outsourcing arrangements. C-suite executives must review and sign-off prior to submission to BSP. Please indicate specific references (e.g., index, page, section, or title) to supporting documents.

NAME OF BANK / NON-BANK FINANCIAL INSTITUTION (NBFI): _____

DATE ACCOMPLISHED: _____

A. OVERVIEW OF THE OUTSOURCED ACTIVITIES AND SERVICE PROVIDER/S

BSP CHECKLIST	BANKS AND NBFI SELF-ASSESSMENT
1. Name of Technology Service Provider (TSP)	
2. Service commencement date. (MM/DD/YY)	
3. Identify and describe:	
3.a Proposed activities, operations and services to be outsourced; and	
3.b Data to be processed, stored, and accessed by TSP, including the data access methods, and BSFI's information classification standards.	

B. ADDRESSING IT OUTSOURCING RISKS AND OTHER AREAS OF CONCERN

IT OUTSOURCING CONCERNS/RISKS	IMPLEMENTED CONTROLS/COMPLIANCE (Indicate N.A. if Not Applicable)
<i>Determine the extent of compliance with the following:</i>	
1. Legal and Regulatory Compliance, Governance and Risk Management, and Due Diligence	
a. Law on Secrecy of Deposits (R.A. No. 1405)	
b. Foreign Currency Deposit System (R.A. 6426)	
c. Anti-Money Laundering Act (R.A. No. 9160, as amended), particularly on data/ file retention	
d. Electronic Commerce Act (R.A. 8792)	
e. Data Privacy Law (R.A. 10173)	
f. Cybercrime Prevention Act (R.A. 10175)	

IT OUTSOURCING CONCERNS/RISKS	IMPLEMENTED CONTROLS/COMPLIANCE (Indicate N.A. if Not Applicable)
g. General Banking Law (R.A. 8791)	
h. Electronic Banking Services (BSP Circular 1033)	
i. Consumer Protection (BSP Circular 1048)	
2. Governance and Risk Management	
a. Adoption of written, board-approved outsourcing policy. Please provide details on policy title, Board approval and last review date	
b. Risk assessment procedure, results and justification in pursuing a technology outsourcing engagement	
c. BSFI's internal audit role/involvement prior to and after the engagement of a TSP	
3. Due Diligence	
Formally defined and documented TSP selection process. Provide briefly the following: a. Selection Criteria b. Considerations for other vendors/service providers c. Reason for choosing the TSP	
4. Vendor Management, Performance and Support	
a. BSFI's monitoring process to manage the outsourced IT service	
b. Process to audit TSP to assess its compliance with entity's policy, procedures, security controls and regulatory requirements	
c. BSFI's procedures in identifying, reporting, and responding to security incidents and violations	
d. BSFI's contingency plan for replacing the TSP in the event of its cessation	
5. Security and Privacy	
a. Information security policies and initiatives to incorporate activities outsourced to TSP and risks pertaining to compromise of confidential/sensitive information processed and/or stored by the TSP.	
b. A comprehensive data inventory and a suitable data classification process to facilitate TSP's implementation of identity and access controls	

IT OUTSOURCING CONCERNS/RISKS	IMPLEMENTED CONTROLS/COMPLIANCE (Indicate N.A. if Not Applicable)
c. Monitoring and management for integrity checking, compliance checking, security monitoring, comprehensive incident response methodologies, and network performance	
d. Procedures established to securely destroy or remove the data when the need arises (e.g., upon contract termination, either on expiry or prematurely)	
6. Business Continuity Planning	
a. Responsibilities and procedures for availability, data backup, incident response and recovery, Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO) of systems or applications outsourced	
b. Frequency of business continuity and disaster recovery tests, validation process and testing methodology	
c. Contingency plan for replacing the TSP in the event of its cessation	

C. COMPLIANCE WITH THE REVISED OUTSOURCING FRAMEWORK

PROVISIONS OF 112 OF THE MORB	SPECIFIC CONTRACT PROVISION/S
The Memorandum of Agreement (MOA)/Service Level Agreement (SLA) has been reviewed and ascertained by a legal counsel to include all pertinent provisions stated in the revised outsourcing framework. Provide the following details: 1. Reviewer 2. Review Date 3. Results of Review	

Master Service Agreement or contract between the bank/NBFI and the service provider, which shall, at a minimum, include all of the following:	
a. Complete description of the work to be performed or services to be provided;	
b. Fee structure;	
c. Provisions governing amendment and pre- termination of contract;	
d. Responsibility, fines, penalties, and accountability of the service provider for errors, omissions and frauds;	
e. Confidentiality clause covering all data and information; solidarity liability of service provider and bank/NBFI for any violation of R.A. No. 1405, (the Bank Deposits Secrecy Law) actions that the bank/NBFI may take against the service provider for breach of confidentiality or any form of disclosure of confidential information; and the applicable penalties;	
f. Segregation of the data of the bank/NBFI from that of the service provider and its other clients;	
g. Disaster recovery/business continuity contingency plans and procedures;	
h. Guarantee that the service provider will provide necessary levels of transition assistance if the bank/NBFI decides to convert to other service providers or other arrangements;	
i. Access to the financial information of the service provider;	
j. Access of internal and external auditors to information regarding the outsourced activities/ services which they need to fulfill their respective responsibilities;	
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 in the event that results of alternative audit mechanism and third-party validation do not satisfy requirements and examination objectives of the regulator/s;	
l. Provision which requires the service provider to promptly 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;	
m. Remedies for the bank/NBFI in the event of change of ownership, assignment, attachment of assets, insolvency, or receivership of the service provider; and	
n. Provision allowing the bank/NBFI to cancel the contract by contractual notice of dismissal or extraordinary notice of cancellation if so required by the Bangko Sentral due to non-compliance with regulatory requirements.	
Additional Requirements for IT Outsourcing:	
o. Provisions regarding on-line communication availability, transmission line security, and transaction authentication;	
p. Responsibilities regarding hardware, software and infrastructure upgrades;	
q. Mandatory notification by the service provider of all systems changes that will affect the bank/NBFI;	
r. Details of all security procedures and standards;	
s. Adequate general insurance coverage (e.g., fidelity and fire liability), if applicable; and	
t. Ownership/maintenance of the computer hardware, software (program source code), user and system documentation, master and transaction data files.	

IT OUTSOURCING QUESTIONNAIRE FOR TSP
Compliance with Section 112 and Appendix 78 of the Manual of Regulations for Banks (MORB) and Appendix Q-65 of
the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI)
on IT Outsourcing/Vendor Management

Note: This self-assessment should be maintained by high-level officers who have direct understanding of the institution's outsourcing arrangements. C-suite executives must review and sign-off prior to submission to BSP. Please indicate specific references (e.g., index, page, section, or title) to supporting documents.

NAME OF TECHNOLOGY SERVICE PROVIDER (TSP): _____

DATE ACCOMPLISHED: _____

A. OVERVIEW OF THE OUTSOURCED ACTIVITIES AND SERVICE PROVIDER/S

BSP CHECKLIST	BANKS AND NBFIs SELF-ASSESSMENT
1. Provide brief description on the company profile: a. History b. Location c. Business purpose and services offered d. Credibility and Certifications e. Partners, affiliates, and sub-vendors f. Contact Information and website	
2. Service commencement date. (MM/DD/YY)	
3. Identify and describe:	
3.a Proposed services to be provided	
3.b Data to be processed/stored and its information classification standards	

B. ADDRESSING IT OUTSOURCING RISKS AND OTHER AREAS OF CONCERN

IT OUTSOURCING CONCERNS/RISKS	IMPLEMENTED CONTROLS/COMPLIANCE (Indicate N.A. if Not Applicable)
1. Vendor Management, Performance and Support	
a. Clear disclosure on the Service Level Agreement (SLA) of other parties (i.e., subcontractors) that are involved in the delivery of IT	

IT OUTSOURCING CONCERNS/RISKS	IMPLEMENTED CONTROLS/COMPLIANCE (Indicate N.A. if Not Applicable)
services. Please provide background information of all vendors/subcontractors that are in critical path of the TSP	
b. TSP's guarantee of availability and extent of liability if SLAs are not met	
c. Grant of BSP access to TSP's operations in the event that results of alternative audit mechanism and third-party validation do not satisfy requirements and examination objectives of the regulators.	
d. TSP's procedures in identifying, reporting, and responding to operational incidents and violations and its involvement in providing support to the BSFI	
2. Security and Privacy	
a. A comprehensive data inventory and a suitable data classification process to facilitate TSP's implementation of identity and access controls	
b. Implementation of adequate security controls and procedures to protect storage and transmission of confidential or sensitive information/data between hosts and terminals. Include discussion on: • Security features • Information and cyber security controls. • End-to-end encryption	
c. For cloud outsourcing, the location of primary and secondary sites and physical and environmental controls in place	
d. Monitoring and management for integrity checking, compliance checking, security monitoring, comprehensive security incident response methodologies, and network performance	
e. Procedures established to securely destroy or remove the data when the need arises (e.g., upon contract termination, either on expiry or prematurely) and validate proper data purge	

3. Data Ownership and Data Location and Retrieval	
a. Location where data/information is stored and the extent of control over those data/information	
b. Clear stipulation of legal ownership rights over the data to enable a basis for trust and privacy of data	
c. Data segregation and isolation from other subscriber's data	
4. Business Continuity Planning	
a. Responsibilities and procedures for availability, data backup, incident response and recovery, Recovery Time Objectives (RTO), and recovery point objectives (RPO) of systems or applications outsourced	
b. Prioritization arrangements in case of multiple/simultaneous disasters	
c. Frequency of business continuity and disaster recovery tests, validation process and testing methodology	
5. Audit and Security Reviews	
a. TSP's audit solutions that will allow BSFIs to perform audit and compliance review of their IT security configurations, in the event that alternative audit mechanisms are deemed insufficient	
b. Periodic independent security audits/reviews (Discuss briefly)	
c. In relation to the previous item, list down all the security reports conducted in the past year and indicate the following information: i. Name of report/s ii. Brief description iii. Assessment/audit scope iv. Date/s conducted v. Conducted by vi. Audit rating/results	