IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: IT Outsourcing/Vendor Management
(Appendix to Sec. 148 on Purpose and Scope, and IT Risk Management Systems)

1. INTRODUCTION

1.1. With globalization and advancement in IT, BSFIs increasingly rely on services provided by other entities to support an array of IT-related functions. The ability to outsource IT systems and process enables a BSFI to manage costs, obtain necessary expertise, expand customer product offerings, and improve services. While outsourcing offers a cost-effective alternative to in-house capabilities, it does not reduce the fundamental risks associated with IT or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information and regulatory action remain. Because the functions are performed by an organization outside the BSFI, the risks may be realized in a different manner than if the functions were inside resulting in the need for well-structured process to properly manage risks and ensure that the interest of customers will not be compromised.

2. ROLES AND RESPONSIBILITIES

2.1. **Board of Directors (Board) and Senior Management.** The responsibility for the oversight and management of outsourcing activities and accountability for all outsourcing decisions continue to rest with the BSFI's Board and senior management. They should establish and approve enterprise-wide policies, appropriate to the IT risk profile of the institution. This framework should govern the end-to-end perspective of outsourcing process and shall provide the basis for management to identify, measure, monitor, and control the risks associated with IT-related outsourcing arrangements.

3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM

3.1 **Risk Assessment.** Prior to entering into an outsourcing plan, the BSFI should clearly define the business requirements for the functions or activities to be outsourced, assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks. Risk assessment should take into consideration the criticality of the services to be outsourced, the capability of the technology service provider (TSP)[1] and the technology it will use in delivering the outsourced service. Such assessment should be made periodically on existing arrangements as part of the outsourcing program and review process of the BSFI.

3.2 **Service Provider Selection.** Before selecting a service provider, the BSFI should perform appropriate due diligence of the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity in relation to the services to be outsourced. The depth and formality of the due diligence performed may vary depending on the nature of the outsourcing arrangement and the BSFI's familiarity with the prospective service providers. Contract negotiation should be initiated with the service provider determined to best meet the business requirements of the BSFI.

Due diligence undertaken during the selection process should be documented and reviewed periodically, using the most recent information, as part of the monitoring and control processes of outsourcing.

3.3 Outsourcing Contracts. The contract is the legally binding document that defines all aspects of the servicing relationship and one of the most important controls in outsourcing process. It should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality and reporting. Before signing a contract, management should:

a. Ensure the contract clearly defines the rights and responsibilities of both parties and contains or supported by adequate and measurable service level agreements;

b. Ensure contracts with related entities clearly reflect an arms-length relationship and costs and services are on terms that are substantially the same, or at least as favorable to the BSFI, as those prevailing at the time for comparable transactions with non- related third parties;

c. Choose the most appropriate pricing method for the BSFI's needs;

d. Ensure service provider's physical and data security standards meet or exceed the BSFI's standards. Any breach in security should be reported by the service provider to the BSFI;

e. Engage legal counsel to review the contract; and

f. Ensure the contract contains the minimum provisions required under existing Bangko Sentral rules and regulations, like access by Bangko Sentral to systems and databases outsourced, and the same does not include any provisions or inducements that may adversely affect the BSFI (i.e. extended terms, significant increases after the first few years, substantial cancellation penalties).

Each agreement should allow for renegotiation and renewal to enable the BSFI to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet its legal and regulatory obligations. The agreement should also acknowledge Bangko Sentral's supervisory authority over the BSFI and the right of access to information on the BSFI and the service provider.

Some service providers may contract with third-parties in providing IT services to the BSFI. The extent to which subcontractors perform additional services should be limited to peripheral or support functions while the core services should rest with the main service provider. The BSFI should retain the ability to maintain similar control over its outsourcing risks when a service provider uses subcontractors in the course of rendering the IT-related services. Agreements should have clauses setting out the rules and limitations on subcontracting. To provide accountability, it may be beneficial for the BSFI to include a provision specifying that the contracting service provider shall remain fully responsible with respect to parts of the services which were further outsourced to subcontractors. It should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.

An annual review of the outsourcing agreements should be performed to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies. When renegotiating contracts, the BSFI should ensure that the provider delivers a level of service that meets the needs of the institution over the life of the contract.

3.4 **Service Level Agreement (SLA).** SLAs formalize the performance standards against which the quantity and quality of service should be measured. Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability for the outsourced activity. The BSFI should link SLA to the provisions in the contract regarding incentives, penalties and contract cancellation in order to protect themselves in the event the service provider failed to meet the required level of performance.

Management should closely monitor the service provider's compliance with key SLA provision on the following aspects, among others:

a. Availability and timeliness of services;
b. Confidentiality and integrity of data;
c. Change control;
d. Security standards compliance, including vulnerability and penetration management;
e. Business continuity compliance; and

f. Help desk support.

SLAs addressing business continuity should measure the service provider's contractual responsibility for backup, record retention, data protection, and maintenance and testing of disaster recovery and contingency plans. Neither contracts nor SLAs should contain any extraordinary provisions that would exempt the service provider from implementing its contingency plans (outsourcing contracts should include clauses that discuss unforeseen events for which the BSFI would not be able to adequately prepare).

3.5 **Ongoing Monitoring**

3.5.1. Monitoring Program. As outsourcing relationships and interdependencies increase in materiality and complexity, the BSFI needs to be more proactive in managing its outsourcing relationships. It should establish a monitoring program to ensure service providers deliver the quantity and quality of services required by the contract. The resources to support this program will vary depending on the criticality and complexity of the system, process, or service being outsourced.

The program should employ effective mechanisms to monitor key aspects of the outsourcing relationship and the risk associated with the outsourced activity, particularly the following:

a. contract/SLA performance;
b. material problems encountered by the service provider which may impact the BSFI;
c. financial condition and risk profile; and
d. business continuity plan, the results of testing thereof and the scope for improving it.

To increase the effectiveness of monitoring mechanisms, management should periodically classify service provider relationships to determine which service providers require closer monitoring. Relationships with higher risk classification should receive more frequent and stringent monitoring for due diligence, performance (financial and/or operational), and independent control validation reviews.

Personnel responsible for monitoring activities should have the necessary expertise to assess the risks and should maintain adequate documentation of the process and results thereof. Management should use such documentation when renegotiating contracts as well as developing business continuity planning requirements.

Reports on the monitoring and control activities of the BSFI should be prepared or reviewed by its senior management and provided to its Board. The BSFI should also ensure that any adverse development arising from any outsourced activity is brought to the attention of the senior management, or the Board, when warranted, on a timely basis. Actions should be taken to review the outsourcing relationship for modification or termination of the agreement.

3.5.2. **Financial Condition of Service Providers.** The BSFI should have an on-going monitoring of the financial condition of its service providers as financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession. In the event management recognizes that the financial condition of the provider is declining or unstable, more frequent financial reviews of said provider are warranted.

3.5.3. **General Control Environment of the Service Provider.** The BSFI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their function. Management should restrict their access to BSFI's systems, and appropriate access controls and monitoring should be in place between the service provider's systems and the BSFI.

3.6. **Business Continuity Planning Consideration.** The BSFI should integrate the provider's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications.

3.7. **Compliance with Bangko Sentral Regulations.** The BSFI should ensure that appropriate up-to-date records relevant to its outsourcing arrangements are maintained in its premises and kept available for inspection by the Bangko Sentral Examiners. The outsourcing agreement should explicitly provide a clause allowing Bangko Sentral and BSFIs' internal and external auditors to review the operations and controls of the service provider as they relate to the outsourced activity.

In addition to the general guidelines on outsourcing contracts stated in Item No. "3.3" of this Appendix, the BSFIs intending to outsource must comply with existing Bangko Sentral rules and regulations on outsourcing.

4. EMERGING OUTSOURCING MODELS

4.1. With continued and fast growth of technology, outsourcing of IT-related systems and processes

has been a constant theme among BSFIs. While outsourcing strategy allows BSFIs to achieve growth targets, operational efficiency and cost savings, this also exposes them to various levels and kinds of risks. Potential risk exposures and other significant supervisory concerns are further heightened by the emergence of flexible and innovative outsourcing models (i.e. shared-services, offshoring and cloud computing).

4.2. Due mainly to the perceived implications for greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention. Currently, the most widely accepted definition of cloud computing is as follows –

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[2]

4.3. In general, cloud computing is a migration from owned resources to shared resources in which client users receive IT services, on demand, from third-party service providers a.k.a. Cloud Service Providers (CSP) via the Internet "cloud." This emerging model allows BSFIs the option to move from a capital-intensive approach to a more flexible business model that lowers operational costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The four (4) cloud deployment models include the following:

a. Private Cloud – A private cloud is operated solely for an institution and is closely related to the existing IT outsourcing models in the marketplace, but can be an institution's internal delivery model as well.

b. Public Cloud – A public cloud is owned and operated by a CSP that delivers services to the general public or a large industry group via the internet or other computer network using a multi-tenant platform.

c. Community Cloud – It is a private- public cloud with users having a common connection or affiliation, such as a trade association, the same industry or a common locality. It allows a CSP to provide cloud tools and applications specific to the needs of the community.

d. Hybrid Cloud – This model composes two or more clouds (private, community or public). A hybrid cloud leverages on the advantage of the other cloud models, thus, providing a more optimal user experience.

4.4. Cloud computing is perceived to play an increasingly important role in a wide range of development initiatives, including among others, offering small to medium- sized BSFIs critical access to infrastructure and computational resources that would otherwise be out of their financial reach or are too complex to manage. While the advantages of adopting an outsourced cloud-based component are undeniable, the fact remains that cloud computing also creates disruptive possibilities and potential risks. Many of the threats identified are not necessarily unique to the cloud environment. In fact, risks such as potential data loss, poor management by a service provider, service interruption and unauthorized access to sensitive data are also applicable to traditional forms of outsourcing. Cloud computing, however, adds new dimensions to the traditional outsourcing risks, thus, the vulnerabilities and the probability of the risk event occurring is amplified. BSFIs should be fully aware of the unique attributes and risks associated with cloud computing, particularly in the following areas: (Details are shown in the attached Annex "A")

- o Legal and Regulatory Compliance;
- o Governance and Risk Management;
- o Due Diligence;
- o Vendor Management/Performance and Conformance;
- o Security and Privacy;
- o Data Ownership and Data Location and Retrieval;
- o Business Continuity Planning.

4.5. Among the four (4) cloud models, the private cloud deployment is most similar to traditional outsourcing model, thus, offers the least amount of new risks and security challenges. Implementation of this model is allowed subject to compliance with existing Bangko Sentral rules and regulations on outsourcing. Adoption of community and hybrid cloud deployment models may also be allowed with prior Bangko Sentral approval, subject to the following:

a. Compliance with existing Bangko Sentral rules and regulations on outsourcing;
b. Implementation of more robust risk management systems and controls required for these types of arrangements;
c. Issues set out in the attached Annex "A" are properly addressed prior to executing the plans; and
d. Bangko Sentral may be allowed to perform onsite validation prior to implementing the cloud computing arrangement/s.

4.6. However, given the increased probability of risk & exposure to potential issues related to business operations, confidentiality and compliance which are critical in the financial service industry, the Bangko Sentral, at present, would only allow the use of public cloud computing

model for non-core operations and business processes (e.g., email, office productivity, collaboration tools, claims and legal management, etc.) which do not directly involve sensitive BSFI and customer data. Bangko Sentral approval of public cloud deployment model for non-core operations shall be subject to the same conditions in Item 4.5 above. Core operations and business processes whose importance is fundamental in ensuring continuous and undisturbed operation of IT systems used to directly perform banking and financial services (e.g., CA/SA, Loans, Trust and Treasury systems, ATM switch operations, electronic delivery systems and systems used to record banking operations) are not allowed to use public cloud computing service. Distinguishing whether a particular actual operation or business is "core" or "non-core" and classifying the data (e.g. confidential, critical, sensitive, public) associated with the system or application are, therefore, significant considerations in determining permissibility of public cloud model for this type of operation or process.

4.7. BSFIs should consult Bangko Sentral before making any significant commitment on cloud computing.

5. ROLE OF IT AUDIT

5.1. The BSFI should conduct a regular, comprehensive audit of its service provider relationships. The audit scope should include a review of controls and operating procedures that help protect the BSFI from losses due to irregularities and willful manipulations. Such responsibility can be assigned to the BSFI's IT audit function. In case the BSFI has no technical audit expertise, the non-technical audit methods can provide minimum coverage and should be supplemented with comprehensive external IT audits.

(Circular No. 958 dated 25 April 2017)

ANNEX A

Despite its many potential benefits, cloud computing also brings with it potential areas of concern, when compared with computing environments found in traditional data centers. Some of the more fundamental concerns include the following:

1. **Legal and Regulatory Compliance**

Important considerations for any BSFI before deploying a cloud computing model include clearly understanding the various types of laws and regulations that potentially impact cloud computing initiatives, particularly those involving confidentiality, visibility, data location, privacy

and security controls and records management. The nature of cloud computing may increase the complexity of compliance with applicable laws and regulations because customer data may be stored or processed offshore. The BSFI's ability to assess compliance may be more complex and difficult in an environment where the Cloud Service Provider (CSP) processes and stores data overseas or comingles the BSFI's data with data from other customers that operate under diverse legal and regulatory jurisdictions. The BSFI should understand the applicability of local laws and regulations and ensure its contract with a CSP specify its obligations with respect to the BSFIs' responsibilities for compliance with relevant laws and regulations. CSP's processes should not compromise compliance with the following, among others:

a. Law on Secrecy of Deposits (R.A. No. 1405);
b. Foreign Currency Deposit System (R.A. No. 6426)
c. Anti-Money Laundering Act, particularly on data/file retention;
d. Electronic Commerce Act (R.A. No. 8792);
e. Data Privacy Law;
f. Cybercrime Prevention Act;
g. General Banking Law (R.A. No. 8791); and
h. Regulations concerning IT risk management, electronic banking, consumer protection, reporting of security incidents and other applicable Bangko Sentral issuances, rules and regulations.

Lastly, the CSP should grant Bangko Sentral access to its cloud infrastructure to determine compliance with applicable laws and regulations and assess soundness of risk management processes and controls in place.

2. **Governance and Risk Management**

The use of outsourced cloud services to achieve the BSFI's strategic plan does not diminish the responsibility of the Board of Directors and management to ensure that the outsourced activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations. The BSFI Management should consider overall business and strategic objectives prior to outsourcing the specific IT operations to the cloud computing platform. A Board-approved outsourcing policy and rationale for outsourcing to the cloud environment should be in place to ensure that the Board is fully apprised of all the risks identified.

Outsourcing to a CSP can be advantageous to a BSFI because of potential benefits such as cost reduction, flexibility, scalability, improved load balancing, and speed. However, assessing and managing risk in systems that use cloud services can be a formidable challenge due mainly to the unique attributes and risks associated with a cloud environment especially in areas of

data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality as well as legal issues such as regulatory compliance, auditing and data offshoring. Cloud computing may require more robust controls due to the nature of the service. When evaluating the feasibility of outsourcing to a CSP, it is important to look beyond potential benefits and to perform a thorough due diligence and risk assessment of elements specific to the service. Vendor management, information security, audits, legal and regulatory compliance, and business continuity planning are key elements of sound risk management and risk mitigation controls for cloud computing. As with other service provider offerings, cloud computing may not be appropriate for all BSFIs.

3. **Due Diligence**

The due diligence in selecting a qualified CSP is of paramount importance to ensure that it is capable of meeting the BSFI's requirements in terms of cost, quality of service, compliance with regulatory requirements and risk management. Competence, infrastructure, experience, track record, financial strength should all be factors to consider. When contemplating transferring critical organizational data to the cloud computing platform, it is critical to understand who and where all of the companies and individuals that may touch the BSFI's data. This includes not only the CSP, but all vendors or partners that are in the critical path of the CSP. Background checks on these companies are important to ensure that data are not being hosted by an organization that does not uphold confidentiality of information or that is engaging in malicious or fraudulent activity. Business resiliency and capability to address the BSFI's requirements for security and internal controls, audit, reporting and monitoring should also be carefully considered.

4. **Vendor Management/Performance and Conformance**

It is always important to thoroughly review the potential CSP's contract terms, conditions and SLA. This is to ensure that the CSP can legally offer what it has verbally committed to and that the cloud risk from the CSP's service offerings is within the determined level of acceptable risk of the BSFI. The SLA should ensure adequate protection of information and have details on joint control frameworks. It should also define expectations regarding handling, usage, storage and availability of information, and specify each party's requirements for business continuity and disaster recovery. At a minimum, the SLA should cover the provisions required under existing rules and regulations on outsourcing.

A vendor management process should be in place that proactively monitors the performance of the CSP on an ongoing basis. This is also to guarantee availability and reliability of the services provided and ability to provide consistent quality of service to support normal and peak business requirements. If a BSFI is using its own data centre, it can mitigate and prepare for

outages. However, if it is using a cloud computing service, it has to put all its trust in the cloud service provider delivering on its SLA. This requires that SLA has sufficient means to allow transparency into the way a CSP operates, including the provisioning of composite services which is a vital ingredient for effective oversight of system security and privacy by the BSFI.

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Collection and analysis of available data about the state of the system should be done regularly and as often as needed by the BSFI to manage security and privacy risks, as appropriate for each level of the organization involved in decision making. Transition to public cloud services entails a transfer of responsibility to the CSP for securing portions of the system on which the BSFI's data and applications operate. To fulfill the obligations of continuous monitoring, the organization is dependent on the CSP, whose cooperation is essential, since critical aspects of the computing environment are under its complete control.

Cloud services that allow CSP to further outsource or subcontract some of its services may also heighten concerns, including the scope of control over the subcontractor, the responsibilities involved (e.g., policy and licensing arrangements), and the remedies and recourse available should problems occur. A CSP that hosts applications or services of other parties may involve other domains of control, but through transparent authentication mechanisms, appear to the BSFI to be that of the CSP. Requiring advanced disclosure of subcontracting arrangements, and maintaining the terms of these arrangements throughout the agreement or until sufficient notification can be given of any anticipated changes, should be properly enforced.

Additionally, the complexity of a cloud service can obscure recognition and analysis of incidents. The CSP's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Each layer in a cloud application stack, including the application, operating system, network, and database, generates event logs, as do other cloud components, such as load balancers and intrusion detection systems; many such event sources and the means of accessing them are under the control of the cloud provider. It is important that the CSP has a transparent response process and mechanisms to share information with the BSFI during and after the incident. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought. The geographic location of data is a related issue that can impede an investigation, and is a relevant subject for contract discussions. Revising the BSFI's incident response plan to address differences between the organizational computing environment and the cloud computing environment is also a prerequisite to transitioning applications and data to the cloud.

Lastly, to effectively monitor services including risk and risk mitigation associated with the use of a CSP, the BSFI and the CSP should agree in advance that former shall have accessibility to the CSP to audit and verify the existence and effectiveness of internal and security controls specified in the SLA. The BSFI's audit policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing. It may also be necessary to augment the internal audit staff with additional training and personnel with sufficient expertise in evaluating shared environments and virtualized technologies. In addition, the parties may also agree on the right to audit clause via external party as a way to validate other control aspects that are not otherwise accessible or assessable by the BSFI's own audit staff. Ideally, the BSFI should have control over aspects of the means of visibility to accommodate its needs, such as the threshold for alerts and notifications, and the level of detail and schedule of reports.

5. **Security and Privacy**

Security and privacy concerns continue to be a major issue within a cloud computing model. Given the obvious sensitivity of data and the regulated environment within which they operate, BSFIs utilizing cloud systems, need to have an assurance that any data exposed on the cloud is well protected. They may need to revise their information security policies, standards, and practices to incorporate the activities related to a CSP. They should also have an understanding of and detailed contracts with SLAs that provide the desired level of security to ensure that the CSP is applying appropriate controls. In certain situations, continuous monitoring of security infrastructure may be necessary for BSFIs to have a sufficient level of assurance that the CSP is maintaining effective controls.

It is important that BSFIs maintain a comprehensive data inventory and a suitable data classification process, and that access to customer data is restricted appropriately through effective identity and access management. A multi-tenant cloud deployment, in which multiple clients share network resources, increases the need for data protection through encryption and additional controls such as virtualization mechanisms to address the risk of collating organizational data with that of other organizations and compromising confidential information through third-party access to sensitive information. Verifying the data handling procedures, adequacy and availability of backup data, and whether multiple service providers are sharing facilities are important considerations. If the BSFI is not sure that its data are satisfactorily protected and access to them is appropriately controlled, entering into a cloud service arrangement may not be suitable.

Storage of data in the cloud could increase the frequency and complexity of security incidents. Therefore, management processes of the BSFI should include appropriate notification procedures; effective monitoring of security-related threats, incidents and events on both BSFI's

and CSP's networks; comprehensive incident response methodologies; and maintenance of appropriate forensic strategies for investigation and evidence collection.

6. **Data Ownership and Data Location and Retrieval**

The BSFI's ownership rights over the data must be firmly established in the contract to enable a basis for trust and privacy of data. Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the CSP acquires no rights or licenses through the agreement, to use the BSFI's data for its own purposes; and that the CSP does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the CSP.

One of the most common challenges in a cloud computing environment is data location. Use of an in-house computing center allows the BSFI to structure its computing environment and to know in detail where data is stored and what safeguards are used to protect the data. In contrast, the dynamic nature of cloud computing may result in confusion as to where information actually resides (or is transitioning through) at a given point in time, since multiple physical locations may be involved in the process. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. One of the main compliance concerns is the possible transborder flows of data which may impinge upon varying laws and regulations of different jurisdictions.

To address the above constraints, the BSFI should pay attention to the CSP's ability to isolate and clearly identify its customer data and other information system assets for protection. Technical, physical and administrative safeguards, such as access controls, often apply. Likewise, such concerns can be alleviated if the CSP has some reliable means to ensure that an organization's data is stored and processed only within specific jurisdictions. Lastly, external audits and security certificates can mitigate the issues to some extent.

7. **Business Continuity Planning**

The BCP in a BSFI involves the recovery, resumption, and maintenance of the critical business functions, including outsourced activities. Due to the dynamic nature of the cloud environment, information may not immediately be located in the event of a disaster. Hence, it is critical to ensure the viability of the CSP's business continuity and disaster recovery plans to address broad-based disruptions to its capabilities and infrastructure. The plans must be well documented and tested. Specific responsibilities and procedures for availability, data backup, incident response and recovery should be clearly understood and stipulated. Recovery Time

Objectives should also be clearly stated in the contract. It is critical for the BSFI to understand the existence and comprehensiveness of the CSP's capabilities as well as its level of maturity to ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner. Other BCP-related concerns which must be addressed by the BSFI and CSP include the following:

a. Prioritization arrangements in case of multiple/simultaneous disasters;
b. Retention of onsite and offsite back- up (Whether to maintain an up-to-date back- up copy of data at the BSFI's premises or stored with a second vendor that has no common points of failure with the CSP); and
c. Ability to synchronize documents and process data while the client-BSFI is offline.

(Circular No. 958 dated 25 April 2017)

Footnotes

1. *TSPs* include a wide range of entities including but not limited to affiliated entities, non-affiliated entities, and alliances of companies providing technology products and services. These services may include but not limited to the following: a) information and transaction processing and settlement activities that support banking functions; b) electronic banking-related services; c) Internet-related services; d) security monitoring; e) systems development and maintenance; f) aggregation services; and g) digital certification services. Other terms used to describe TSPs include vendors and external/outsourced service providers.
2. National Institute of Standards Technology, *The NIST Definition of Cloud Computing: Special Publication 800-145, 2011, www.nist.gov/itl/cloud/*