website: www.bb.org.bd

ব্যাংকিং প্রবিধি ও নীতি বিভাগ
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা।

বিআরপিডি সার্কুলার নং-০৫

তারিখ ঃ ০২ চৈত্র ১৪২৯ / ১৬ মার্চ ২০২৩

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল তফসিলি ব্যাংক/ অ-ব্যাংক আর্থিক প্রতিষ্ঠান/মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রোভাইডার/পেমেন্ট সার্ভিস প্রোভাইডার/ পেমেন্ট সিস্টেম অপারেটর এবং অন্যান্য আর্থিক সেবা প্রদানকারী প্রতিষ্ঠান।

প্রিয় মহোদয়,

Guidelines on Cloud Computing

আর্থিক খাতে উন্নত প্রযুক্তি ব্যবহারের মাধ্যমে ডিজিটাল বাংলাদেশ গঠনে দেশ এগিয়ে যাচ্ছে। বর্তমানে স্মার্ট বাংলাদেশ বিনির্মাণের লক্ষ্যে আর্থিক খাতে ব্যবহৃত সিস্টেমসমূহ পরিচালনায় তথ্য সংরক্ষণ ও প্রক্রিয়াকরণসহ বিভিন্ন ক্ষেত্রে উচ্চ গতির ইন্টারনেট ও ক্লাউড কম্পিউটিং প্রযুক্তি ব্যবহারের প্রবণতা লক্ষ্যণীয়। চাহিদানুযায়ী সর্বোৎকৃষ্ট প্রযুক্তি ব্যবহার, ব্যয় সাশ্রয়, যেকোন সময় যেকোন স্থান হতে সিস্টেমে প্রবেশের সুযোগ, সিস্টেম ব্যবহারে নিরবচ্ছিন্নতা এবং উন্নত নিরাপত্তা ব্যবস্থার কারণে ক্লাউড সেবা গ্রহণের হারও প্রতিনিয়ত বৃদ্ধি পাচ্ছে। তবে, ক্লাউড কম্পিউটিং প্রযুক্তি ইন্টারনেট নির্ভর হওয়ায় এতে সাইবার আক্রমণসহ তথ্যের গোপনীয়তা ও নিরাপত্তা সংক্রান্ত ঝুঁকি রয়েছে। সামগ্রিকভাবে আর্থিক খাতে স্থিতিশীলতা বজায় রাখার লক্ষ্যে ক্লাউড কম্পিউটিংয়ের ঝুঁকি নিরূপণ ও কার্যকর তদারকি খুবই গুরুত্বপূর্ণ।

২। এক্ষণে, ক্লাউড সেবার ক্ষেত্র, ক্লাউড অবকাঠামো, ক্লাউড তথ্য ব্যবস্থাপনা, ক্লাউড প্রযুক্তির বাস্তবায়ন, ক্লাউড সেবা গ্রহণের শর্তাবলীসহ ক্লাউড সেবা প্রদানকারীর সার্বিক ব্যবস্থাপনা, ক্লাউড গভর্নেন্স, ক্লাউড সেবা ব্যবহারের ঝুঁকি নিরূপণ, তথ্যের গোপনীয়তা ও নিরাপত্তা নিশ্চিতকরণ, ক্লাউড সংক্রান্ত নিরীক্ষা ও পরিপালন নিশ্চিতকরণ এবং সর্বোপরি ক্লাউড প্রযুক্তির বিষয়ে প্রশিক্ষণ ও সচেতনতা বৃদ্ধি প্রভৃতি বিষয়কে সমন্বিত করে ক্লাউড কম্পিউটিং সংক্রান্ত নীতিমালা "Guidelines on Cloud Computing" জারি করা হলো।

৩। ক্লাউড কম্পিউটিং সংশ্লিষ্ট যেকোন কার্যক্রমের ক্ষেত্রে এ নীতিমালা অনুসরণের জন্য আপনাদেরকে নির্দেশনা প্রদান করা হলো। "Guidelines on Cloud Computing" এ বর্ণিত নির্দেশনার সার্বিক পরিপালন নিশ্চিতসাপেক্ষে ব্যাংক/অ-ব্যাংক আর্থিক প্রতিষ্ঠান/মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রোভাইডার/পেমেন্ট সার্ভিস প্রোভাইডার/পেমেন্ট সিস্টেম অপারেটর এবং অন্যান্য আর্থিক সেবা প্রদানকারী প্রতিষ্ঠান ক্লাউড কম্পিউটিং প্রযুক্তি ব্যবহার করে বিভিন্ন সেবা গ্রহণ করতে পারবে।

৪। বর্তমানে চলমান সকল ক্লাউড সেবা অব্যাহত রাখার ক্ষেত্রে, আগামী ৩১ ডিসেম্বর ২০২৩ তারিখের মধ্যে এ নীতিমালার পরিপালন নিশ্চিত করতে হবে।

৫। অনুচ্ছেদ ৪ -এ বর্ণিত ক্লাউড সেবা গ্রহণকারী ব্যাংক/প্রতিষ্ঠান ব্যতিরেকে অন্যান্য ব্যাংকসহ সকল প্রতিষ্ঠানের জন্য এ নির্দেশনা অবিলম্বে কার্যকর হবে।

৬। Bangladesh Bank Order, 1972 এর 7A(e) অনুচ্ছেদ, ব্যাংক কোম্পানী আইন, ১৯৯১ এর ৪৫ ধারা এবং আর্থিক প্রতিষ্ঠান আইন, ১৯৯৩ এর ১৮(ছ) ধারায় অর্পিত ক্ষমতাবলে এ সার্কুলার জারি করা হলো।

আপনাদের বিশ্বস্ত,

(মোঃ হারুন-অর-রশিদ)
পরিচালক (বিআরপিডি)
ফোন ঃ ৯৫৩০০৯৫

Guidelines on Cloud Computing

Version 1.0

March, 2023

Bangladesh Bank

Technical Committee

Chairman

Mr. Mohammed Ishaque Miah
Systems Manager (Director), Bangladesh Bank

Members

Mr. Jayanta Kumar Bhowmick
Senior Systems Analyst (Additional Director), Bangladesh Bank

Mr. S. M. Tofayel Ahmad,
Systems Analyst (Joint Director) & Member Secretary, Bangladesh Bank

Mr. Fahad Zaman Chowdhury
Senior Maintenance Engineer (Joint Director), Bangladesh Bank

Mr. Md. Ziaul Hoque
Systems Analyst (Joint Director), Bangladesh Bank

Mr. Prakash Chandra Mondal
Systems Analyst (Joint Director), Bangladesh Bank

Mr. Hafiz Al Asad
Assistant Chief Information Security Officer (Joint Director), Bangladesh Bank

Mr. Md. Jakir Hossain
Assistant Systems Analyst (Deputy Director), Bangladesh Bank

Mr. Md. Shafiqul Alam
Deputy Director, Bangladesh Bank

Mr. Jahed Hoshen
Deputy Director, (Ex-Cadre Law), Bangladesh Bank

Mr. TuhinTalukder
Assistant Programmer (Assistant Director), Bangladesh Bank

Mr. Mohammed Rezwan Al Bakhtiar
Chief Information Technology Officer (General Manager), Sonali Bank Ltd.

Mr. Iftekhar Ahmed
Vice President &Technology Head, Citibank, N.A.

Mr. B.M. Zahid ul Haque
Senior Vice President & Chief Information Security Officer (CISO), BRAC Bank Ltd.

Mr. Md. Mushfiqur Rahman
Vice President & Chief Information Security Officer (CISO), First Security Islami Bank Ltd.

Mr. Md. Farhad Rahman
Vice President & Chief Information Security Officer (CISO), HSBC Bangladesh

Mr. A B M Ahasan Ullah
Senior Assistant Vice President, ICT Division, LankaBangla Finance Limited

Table of Contents

Contents

List of Abbreviations

CDN	:	Content Delivery Network
CSP	:	Cloud Service Provider
FaaS	:	Function as-a-Service
IaaS	:	Infrastructure-as-a-Service
ISO	:	International Organization for Standardization
NBFI	:	Non-Bank Financial Institutions
PaaS	:	Platform-as-a-Service
PII	:	Personally Identifiable Information
SaaS	:	Software-as-a-Service
SLA	:	Service Level Agreement

[This page is intentionally left blank]

1. Introduction

1.1 Background

Over the recent years, Cloud Computing has created advantages in scale, resource elasticity, organizational agility, and operational resiliency. Cloud Computing enables banks and other financial institutions to respond rapidly on customer demands for products and experiences.

Trust in an effective financial system is crucial for a fully functioning economy. Cloud Computing is gaining increased use in recent years as Bank, Non-Bank Financial Institution (NBFI), Mobile Financial Service Provider (MFSP), Payment Service Provider (PSP), Payment System Operator (PSO) and other financial service providers seek to get relative easy access to new technologies and also achieve immediate economies of scale. However, the organizations remain accountable for their overall end to end delivery of business activities, including any outsourced components.

From a business strategy perspective, updated applications and platform transformations are significantly simpler on a cloud system. Cloud Computing should be effectively managed to identify risks and monitor any industry concentration to mitigate risks to the overall financial stability of the economy.

1.2 Scope

This guideline is applicable to Bank, NBFI, MFSP, PSP, PSO and other financial service providers. Throughout this guideline all these institutions will be termed together as "**The Organization".**

This guideline addresses the approach and principles necessary for adoption of Cloud Computing by the Organization. However, this guideline does not prescribe or recommend any specific Cloud Computing service, service arrangement, service agreement, service provider or deployment models. The Organization must perform their own analysis to determine if cloud computing meets their strategic aims whilst managing any associated risks and compliance with regulatory requirements.

1.3 Objective

The objectives of this guideline are to establish a minimum baseline for management of Cloud Computing in the Organization based on the following key areas:

a. To ensure proper due diligence while using Cloud Computing.
b. To ensure security and data privacy requirements.
c. To ensure interoperability and portability of data and services between intra-cloud environments.
d. To ensure the roles and responsibilities of the relevant parties.
e. To ensure organizational security, privacy and its computing requirements.
f. To ensure a secure environment for processing of data.
g. To ensure awareness of stakeholders roles and responsibilities for protection of information in cloud environment.
h. To ensure business continuity, resilience and recovery capabilities.
i. To ensure effective Cloud Service Provider (CSP) management.
j. To ensure the best practices (industry standard) of the usage of technology.

1.4 Definition

Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The three main Cloud Computing models are Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Cloud Backup: Cloud backup is the process of backing up data to a remote cloud-based server.

Cloud Broker: A third-party entity (individual or institution) that acts like an intermediary and facilitates the selection of Cloud Computing services on behalf of the Organization.

Cloud Migration: Cloud migration is the process of transferring all of or a part of an organization‟s data, applications, and services from on-premise to the cloud or within the cloud**s**.

Cloud Native: Applications developed specifically for cloud platforms.

Cloud Service Provider (CSP): A Cloud Service Provider (CSP) is a company that offers a Cloud Computing service, such as PaaS, IaaS, or SaaS, to individuals or businesses.

Cloud Sourcing: Cloud sourcing is the act of migrating all or a part of traditional on-premise IT operations to cloud services or within the cloud based services to meet business objectives.

Cloud Storage: Cloud storage is a model of computer storage in which data is stored in facilities (often multiple facilities) managed by a hosting company (Cloud Service Provider) and is accessed remotely by the user via a network.

Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from the Organization that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the Organization in the community, a third party, or some combination of them, and it may exist on or off premises.

Container: A container is a virtualization instance in which the kernel of an operating system allows for multiple isolated user-space instances. Unlike Virtual Machines (VMs), containers do not need to run a full-blown Operating System (OS) image for each instance. Instead, containers are able to run separate instances of an application within a single shared OS.

Content Delivery Network (**CDN**): A Content Delivery Network (CDN) is a network of distributed services that deliver content to a user based on the user‟s geographic proximity to servers. CDNs allow speedy content delivery for websites with high traffic volume or large geographic reach.

Elasticity: In Cloud Computing, elasticity is a term used to reference the ability of a system to adapt to changing workload demand by provisioning and de-provisioning pooled resources so that provisioned resources match current demand.

Extensibility: The ability of a cloud solution to add new runtime and framework support via community build packs.

External Cloud: A private or public customized cloud solution provided by a third-party outside the Organizations to meet client requirements.

Host Machine: A host machine is a piece of physical hardware that hosts virtual machines.

Hybrid Cloud: A hybrid cloud is a Cloud Computing environment that is comprised of a mix of private cloud, public cloud, and on-premises solutions. In a hybrid cloud, private and public cloud infrastructures remain distinct from one another but are bound together by technology that allows data and services portability between them.

Infrastructure as a Service (IaaS): Infrastructure as a Service (IaaS) is a model of Cloud Computing in which the vendor hosts virtualized computing resources, as well as network and storage resources, and provides them to the user as a service via the internet.

Internal Cloud: A Cloud Computing service model that is implemented within the Organizations‟ physical boundaries using dedicated resources and IT infrastructure. It is basically a private cloud instance meant ideally for in-house use.

Managed Service Provider (MSP): A Managed Services Provider (MSP) is an IT services provider that provides fully outsourced network, application, and system services across a network to clients.

Microservices: Microservices or microservice architecture is a way of designing applications in which complex applications are built out of a suite of small, independently deployable services. These „microservices" run their own processes and communicate with one another using lightweight mechanisms such as language-agnostic APIs. Microservices are independently deployable and scalable, and can even be written in different languages.

Multi-Cloud: A multi-cloud strategy is the concurrent use of separate Cloud Service Providers for different infrastructure, platform, or software needs. A multi-cloud approach can help prevent vendor lock-in, and may help an enterprise deal with diverse workloads as well as partners. However, a multi-cloud approach can complicate many processes, such as security and governance, and a Cloud management platform is recommended for this approach.

Multi-Tenancy: Multi-Tenancy is a mode of operation for software in which multiple instances of one or many applications run in a shared environment. In a Cloud Computing model, pooled physical and virtual resources are dynamically assigned and reassigned to tenants according to consumer demand.

On-Demand Self-Service: A Cloud Computing service model by which a customer can provision additional cloud resources on-demand, without involving the service provider. Resources are typically provisioned through an online control panel.

On-Premise Technology: On-Premise technology is software or infrastructure that is run on computers on the premises (in the building) of the person or the Organization using the software or infrastructure.

Platform as a Service (PaaS): Platform as a Service (PaaS) is a model of Cloud Computing in which a vendor provides the hardware and software tools necessary to create, deploy and manage applications at scale to the user via the internet, as a service.

Private Cloud: A private cloud is a cloud infrastructure that is provisioned for use by single organization comprised of multiple users. A private cloud is managed and operated by the organization, a third party, or some combination of them, and it can exist on or off premises.

Public Cloud: A public cloud is a cloud infrastructure that is hosted by cloud services provider and is made available to the public via internet.

Scalability: Scalability is the ability of a process, system, or framework to handle a growing workload. In other words, a scalable system is adaptable to increasing demands. The ability to scale on demand is one of the biggest advantages of Cloud Computing.

Service Level Agreement (SLA): A service level agreement (SLA) is a contractual agreement between a customer and a Service Provider which defines the level of service, availability and performance guaranteed by the Service Provider.

Function as a service (FaaS)/ Serverless Computing: It is a platform for providing compute, storage, and network resources without the need of managing machines. In this execution model, the cloud provider runs the server and dynamically allocates machine resources without worrying about the underlying infrastructure.

Software as a Service (SaaS): Software as a service (SaaS), is a model of Cloud Computing in which applications (software) are hosted by a vendor and provided to the user as a service. SaaS applications are licensed on a subscription basis and are made available to users over a network, typically the internet. Because SaaS applications can be accessed at any time, at any place, and on any platform, they have become a popular model for delivery of many business applications.

Vendor Lock-in: Vendor lock-in is when a customer finds themselves "locked-in" or stuck with a certain Cloud Service Provider (CSP). Vendor lock-in is characterized by extreme difficulty in moving from one cloud vendor to another, usually due to lack of standardized protocols, APIs, data structures, and service models.

Vertical Cloud: A vertical cloud is a Cloud Computing solution that is built or optimized for a specific business vertical such as manufacturing, financial services, or healthcare.

Virtual Desktop Infrastructure (**VDI**): Virtual desktop infrastructure (VDI) is a desktop operating system hosted within a virtual machine.

Virtual Machine (VM): A virtual machine is a software computer that runs an operating system or application environment, just as physical hardware would. The end-user has the same experience on a VM as on dedicated hardware.

Virtual Machine Monitor (VMM): The program that is used to manage processor scheduling and physical memory allocation. It creates virtual machines by partitioning the actual resources, and interfaces the underlying hardware (virtual operating platform) to all operating systems (both host and guest).

2. Cloud Architecture

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

It is the way technology components combine to build a cloud, in which resources are pooled through virtualization technology and shared across a network. The components of a cloud architecture include: a front-end platform (the client or device used to access the cloud), a back-end platform (servers and storage), a cloud-based delivery model, a network.

2.1 Cloud Characteristics

2.1.1 Broad network

2.1.1.1 The Organization shall access the data of the cloud or upload the data to the cloud from permitted locations and authorized secure devices.

2.1.1.2 In case of a broad network, the Organization shall ensure the following security measures:

a) Prevent accidental exposure to network routing and security.
b) Identify and remediate exposed Cloud Computing Platform or service that allow access from "any" source IP address.
c) Restrict management ports for remote connectivity.

2.1.2 On-Demand Self-Service

2.1.2.1 There shall have a mechanism for monitoring all the allotted cloud resources like server uptime, capabilities, and allotted network storage etc.

2.1.2.2 The Organization may automatically request the service based on their needs.

2.1.3 Measured service

2.1.3.1 Cloud Computing shall have the ability to control and optimize resource like storage, processing, bandwidth, and active user accounts etc.

2.1.3.2 The system shall have the capability to monitor and control resource usages.

2.1.3.3 Cloud Computing may support a metering capability at some level of services.

2.1.4 Resource pooling

2.1.4.1 The system shall have the ability to share resources among several systems of client as per business requirements.

2.1.5 Rapid elasticity and scalability

2.1.5.1 The cloud system shall have mechanism to elastically provision and release of computing resources.

2.2 Service Models

Though service-oriented architecture advocates "Everything as a service (EaaS)", cloud-computing providers offer their "services" according to different models, of which the standard models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Desktop as a Service (DaaS), Mobile "backend" as a service (MBaaS), Function as a Service (FaaS), Unified Communications-as-a-Service (UCaaS), Business-Process-as-a-Service (BPaaS), Container as a Service (CaaS), Security as a Service (SecaaS), etc. This guideline describes following major service models:

2.2.1 Software as a Service (SaaS)

2.2.1.1 The applications shall be accessible from permitted locations and authorized secured devices using secure interface (such as web browser, email, application interface, etc.).

2.2.1.2 The Organization shall ensure the following security measures in case of SaaS:

a) Detection of rogue services and compromised accounts
b) Identity and Access Management (IAM)
c) Encryption of cloud data
d) Data Loss Prevention (DLP)
e) Monitoring of collaborative sharing of data
f) Confidentiality, Integrity and Availability of data

2.2.2 Platform as a Service (PaaS)

2.2.2.1 The Organization may develop and/or deploy applications onto the cloud infrastructure using programming languages, databases, libraries, services, and tools supported by the provider.

2.2.2.2 The Organization shall ensure the following security measures in case of PaaS:

a) Perform threat modeling
b) Review the provider's security
c) Analyze inherited software vulnerabilities
d) Implement role-based access controls
e) Manage inactive accounts
f) Security Measures of SaaS Clause 2.2.1.2 will be applicable for PaaS.

2.2.3 Infrastructure as a Service (IaaS)

2.2.3.1 The Organization shall ensure that CSP has provision of processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

2.2.3.2 The Organization may consider the following security measures in case of IaaS:

a) Protect resources by using authentication and access control
b) Secure privileged access
c) Use multiple resources for better availability
d) Maintain security updates to resources
e) Monitor resources‟ performance

f) Ensure encryption of data
g) Maintain secured connectivity
h) Security Measures of SaaS and PaaS will be applicable for IaaS

2.3 Deployment Models

A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access.

2.3.1 Public Cloud

2.3.1.1 The Organization shall classify data before hosting into public cloud.

2.3.1.2 Customers‟ financial and other sensitive data cannot be hosted in cross-border public cloud. In exceptional cases, it may be hosted in cross-border public cloud subject to the prior approval of Bangladesh Bank.

2.3.1.3 The Organization shall have complete visibility and monitoring over resources and systems.

2.3.1.4 The Organization shall have right to audit their resources in the public cloud by internal/external auditors. Bangladesh Bank shall have right to audit the same.

2.3.2 Private Cloud

2.3.2.1 Private cloud shall be owned, managed, and operated by the Organization itself.

2.3.2.2 The Organization shall have complete visibility and monitoring over their systems.

2.3.3 Community Cloud

2.3.3.1 Community cloud infrastructure shall be provisioned for exclusively used by a specific community of consumers considering mission, security requirements, policy, compliance, etc.

2.3.3.2 Community cloud shall be owned, managed, and operated by one or more Organizations in the consortium and located in the area within the country.

2.3.3.3 The Organization shall classify data before hosting into community cloud.

2.3.3.4 The Organization shall have complete visibility and monitoring over the systems.

2.3.3.5 The Organization shall have right to audit their resources in community cloud by internal and external auditors. Bangladesh Bank shall have right to audit the same.

2.3.4 Hybrid Cloud

2.3.4.1 Hybrid cloud infrastructure shall be a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entity.

2.3.4.2 Data classification and sensitivity has to be considered before hosted in cloud.

2.3.4.3 The Organizations shall have complete visibility and monitoring over their systems.

2.3.4.4 The Organization shall have right to audit their resources in the hybrid cloud by internal and external auditors. Bangladesh Bank shall have right to audit the same.

2.3.4.5 Customers‟ financial and other sensitive data cannot be hosted in cross-border hybrid cloud. In exceptional cases, it may be hosted in cross-border hybrid cloud subject to the prior approval of Bangladesh Bank.

3. Cloud Data management

Cloud data management is the implementation of cloud data management platforms and tools, policies, and procedures that give organizations control of their business data, both in the cloud and in setups where data is stored or sourced in a combination of on-premises and cloud applications.

3.1 Data Classification

3.1.1 The Organization shall classify its data before migrating to cloud through a proper risk assessment.

3.1.2 The Organization shall categorize their data such as **private, sensitive, public, financial, etc.** before cloud migration. Data should be categorized by considering the following factors but not limited to:

a) Confidentiality, Integrity and Availability of Data
b) Business Justification
c) Protection of Personal Identifiable Information (PII)
   i. Sensitive PII (Some Examples but not limited to:)
      - National Identification Number (NID)
      - Mailing Address
      - Gender
      - Religion
      - Telephone Number/Mobile Number
      - Date of Birth
      - Driving License Information
      - Passport Information
      - Taxpayer Identification Number(TIN)
      - Credit Card Information
      - Medical Records
      - Biometrics/ Fingerprint
      - Bank Accounts Number
      - Political Interest
      - Criminal history
      - Financial Information, etc.

   ii. Non-Sensitive PII (Some Examples but not limited to :)
      - Full Name
      - Email Address
      - Post Code
      - Place of Birth, etc.

d) Conform with national law, policy, regulation guideline, Act, Order, etc.

3.1.3 Data shall be secured while at rest, in transit, and in use, and access to the data shall be controlled.

3.2 Data Migration

3.2.1 Data shall be sourced and staged into the cloud environment avoiding duplication and fragmentation.

3.2.2 Standard technology (e.g. Creation, preservation, and examination of checksum value) shall be used to maintain the integrity of data.

3.2.3 The Organization shall perform the post migration review to ensure data consistency and integrity.

3.3 Data Privacy

3.3.1 The Organization shall ensure that its customer data is appropriately protected from other tenants of Cloud Service Provider.

3.3.2 The Organization shall be able to segregate that Personally Identifiable Information (PII) or other private /personal data and need to manage those data in line with the Organizational privacy requirements.

3.3.3 Disclosures of PII to third parties shall be recorded including what PII has been disclosed to whom and at what time subject to prior approval from Bangladesh Bank.

3.3.4 Management of data in line with privacy requirements shall involve an assessment of compliance.

3.4 Data Redaction

3.4.1 The Organization may consider the use of appropriate masking where the risk of data confidentiality breach is high. This may also include during testing.

3.5 Data Retention

3.5.1 Information assets shall be retained according to the Organization‟s retention policies, and securely deleted in line with retention policies.

3.6 Data Disposal

3.6.1 The Organization shall have data disposal and archiving policy and procedure for Cloud Computing environment.

3.6.2 A contractual agreement shall be in place stipulating that in the event of service withdrawal its information assets shall be securely transferred, destroyed and certification shall be provided by CSP to the Organization.

4. Cloud Deployment/ Implementation

4.1 Planning

The Organization requires rigorous analysis before acquisition and deployment of Cloud Computing solutions to ensure that business requirements are met in an effective and efficient manner. The following issues should be considered:

4.1.1 A business analysis should be completed and formally documented, including but not limited to:

a) The subject of the activity under consideration for cloud solution with a clear articulation of the objectives, requirements and deliverables;
b) The critical considerations for decision-making including the strategic, economic, commercial, financial, business continuity and management case for the proposed activity.
c) The associated risks and required controls to mitigate and manage those risks;
d) Consideration of alternative solutions or strategies (where appropriate).

4.1.2 The Organization shall assess capacity and performance requirements, including forecasting of future needs based on business requirements along with relevant risk.

4.2 Budgeting

4.2.1 The Organization shall ensure adequate budget for acquisition, deployment, maintenance, operation, and insurance coverage (if applicable and viable) or risk management fund of cloud services.

4.3 Risk Management

4.3.1 The Organization shall establish a risk management framework and conduct appropriate due diligence to manage the risks associated with CSPs as well as their material sub-contracting arrangements.

4.3.2 The Organization shall consider associated risks and required controls to mitigate and manage cloud risks.

4.3.3 A risk assessment shall be performed addressing key operational risk including legal, procurement, technology, information/cyber risk, privacy risk and other relevant risks.

4.3.4 The Organization shall conduct risk assessment periodically.

4.4 Technical deployment

4.4.1 The Organization shall conduct technical assessment and prepare technical design and architecture design document based on service deployment model such as SaaS, PaaS or IaaS, etc.

4.4.2 The Organization shall have the appropriate controls to use production data during testing in non-production environments.

4.4.3 The Organization shall ensure that any pirated or non-licensed software is strictly prohibited in cloud ecosystem.

4.5 Cloud Security

Cloud deployment needs to incorporate the following security requirements:

4.5.1 Infrastructure security

4.5.1.1 The Organization shall implement necessary measures to secure the cloud and on premise environments to mitigate contagion risks.

4.5.1.2 The Organization shall ensure segregated management network.

4.5.1.3 Network access and security controls such as firewalls, Intrusion Prevention System (IPS), advance threat protection, web proxy, etc. shall be implemented to secure on-premise environment from the cloud.

4.5.1.4 Secured Virtual Private Network (VPN) or direct network connection shall be implemented to secure the traffic between the cloud and on-premise environments.

4.5.1.5 The Organization shall monitor and control the access to the cloud services.

4.5.1.6 The Organization shall consider network segregation of workloads based on the type (production, test, development) and purpose (user, server, interface, critical infrastructure segments).

4.5.1.7 The Organization shall regularly review firewall rules and access lists, especially after network or architectural changes.

4.5.1.8 The Organization shall ensure that the CSP must have at least two data centers in different seismic zone.

4.5.1.9 The Organization shall ensure redundant connectivity between cloud and on-premise.

4.5.1.10 The Organization shall ensure the clarification from CSP about the shared responsibility in applicable cases.

4.5.1.11 The Organization shall ensure that the CSP must maintain Distributed Denial-of-Service (DDoS) protection methods.

4.5.2 Identity and Access Management Security

Identity and Access management shall be a paramount consideration when performing a cloud outsourcing arrangement and shall incorporate both technical and business user access management.

4.5.2.1 The owner shall be identified to ensure accountability, and ownership of each role defined.

4.5.2.2 The Organization shall have identity and access management policies and standards to manage the cloud environment.

4.5.2.3 The Organization shall ensure multi-factor authentication during access in cloud services.

4.5.2.4 The Organization shall ensure appropriate strategy where identity and access management reside in the cloud.

4.5.2.5 The Organization shall review the access right periodically.

4.5.2.6 The Organization shall ensure segregation of duties for user access management

4.5.2.7 The Organization shall ensure Privileged Access Management (PAM) control.

4.5.2.8 The Organization shall ensure break glass procedure or similar mechanism as required.

4.5.2.9 There shall be a mechanism in place to detect when unauthorized accounts are created.

4.5.3 Encryption and Key Management Security

4.5.3.1 The Organization shall ensure that appropriate cryptographic key management is in place, as well as validate the CSP‟s ability to restore the service from backups effectively.

4.5.3.2 The Organization shall ensure that the cloud service provider has formalized and tested processes and systems in place to securely generate and manage cryptographic keys in line with the Organization s requirements.

4.5.3.3 The data at rest on the cloud and in transit shall be encrypted as per the Organization‟s requirement.

4.5.3.4 CSP shall ensure standard encryption algorithm for data at rest and data in transit.

4.5.3.5 Sensitive data including data backups shall be subject to appropriate encryption controls both in-transit and at-rest.

4.5.3.6 Encryption keys used for the encryption of the Organization‟s data shall be unique and not shared with others.

4.5.4 Application Security

4.5.4.1 The Organization shall follow the related controls of Bangladesh Bank‟s ICT Security Guidelines for Bank or FIs for application security.

4.5.4.2 The Organization shall ensure secure coding standard is being practiced for application development.

4.5.4.3 All security related testing, vulnerability assessment and subsequent remedial measures shall be confirmed before application deployment.

4.5.5 Process Security

4.5.5.1 The Organization shall consider procedures including the roles and responsibilities for emergency and standard changes in agreed manner among stakeholders within defined change timeline for patching and software releases.

4.5.5.2 The Organization may include defined conditions and scenarios that allow automated testing and releases where Development and Operations (DevOps) practices are being used.

4.5.5.3 The Organization shall ensure audit trail, record of the changes and evidence.

4.5.5.4 The Organization shall ensure proper testing before deployment of changes. Also testing needs to be documented and evidenced the test cases with sign-off.

4.5.5.5 The Organization shall conduct Post Implementation Review (PIR) where critical business functions may be impacted.

4.5.5.6 For delegation of admin/approver roles, there shall be a management approval process especially for critical or transactional systems.

4.6 Cloud Security Monitoring

4.6.1 The Organization shall ensure that CSP has the provision of security monitoring for adopted cloud services.

4.6.2 The Organization shall consider a secure and robust log maintaining and monitoring system is in place.

4.6.3 The Organization shall ensure that CSP will store the log for at least 2(two) years and the CSP will provide the client with a Graphical User Interface (GUI) to access it.

4.6.4 The Organization may consider the use of advanced security analytics tools for detection of potential anomalies in the cloud environment.

4.7 Cloud Operation and Maintenance

4.7.1 Notification

4.7.1.1 The Organization shall ensure that CSP has appropriate mechanisms to enable notification of changes, or potential disruption of services in advance and within an adequate time frame.

4.7.1.2 The Organization shall ensure the visibility of changes that may impact the operation of its critical services.

4.7.2 Maintenance

4.7.2.1 The Organization shall maintain appropriate system documentations.

4.7.2.2 The Organization shall maintain appropriate asset inventory.

4.7.2.3 The Organization shall maintain environmental baselines, establish a process to review the baselines periodically and monitor deviations from the baselines and take appropriate measures to handle accordingly.

4.7.3 Patching

4.7.3.1 The Organization shall ensure that required patches are implemented and updated.

4.8 Business Continuity and Disaster Recovery

4.8.1 The Organization shall follow related controls of Bangladesh Bank‟s ICT Security Guidelines for Banks and NBFIs to address the business continuity and disaster recovery.

4.8.2 The Organization shall ensure that the Cloud Service Provider maintains two sites (primary site and secondary site) at a minimum considering different seismic zone to ensure availability of services.

4.8.3 The Organization shall ensure a data backup and restore plan for all critical information.

5. Cloud Service Provider (CSP) Management

5.1 Supply Chain Management

5.1.1 The Organization shall seek an inventory of relevant supply chain relationships of CSP.

5.1.2 The Organization shall ensure that CSP periodically reviews risk factors associated with the relevant supply chain.

5.1.3 Monitoring of key services based on SLAs shall be in place and regularly reviewed by the Organization to identify usage anomalies.

5.2 Contractual considerations

5.2.1 The Organization shall ensure CSPs‟ employees possesses required skill and experiences in technical competence and background.

5.2.2 The Organization shall ensure CSP and its subcontractors undertaking any part of the outsourcing arrangement shall be assessed to be fit and proper considering following criteria:

a) They have not been subjected to any proceedings of a disciplinary or criminal nature;
b) They are not involved in any civil liability for fraud or misrepresentation;
c) They have not been convicted of any offense;
d) They are financially sound and transparent;

5.2.3 The Organization shall ensure that the CSP‟s employees are given sufficient training in particular safeguarding of data and security awareness.

5.2.4 All aspects of CSP evaluation process shall be objectively and impartially assessed with due diligence which includes at least:

a) evaluation of experience
b) capability to deliver performance
c) security/privacy requirements
d) financial strength
e) corporate governance and internal control
f) business continuity and disaster recovery
g) external environment (such as economic, social and legal environment of the jurisdiction in which the service provider operates)
h) track record and ability to comply with applicable laws and regulations including privacy laws in all relevant jurisdictions

5.2.5 The Organization shall ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements.

5.2.6 The contractual negotiation shall include a process to ensure that regulatory requirements are captured within the written agreement. The agreement shall also include the following aspects:

a) scope of arrangement
b) performance, operational, internal control and risk management standards

c) security and privacy
d) business continuity management
e) monitoring and control
f) audit and inspection
g) notification of adverse developments
h) dispute resolution
i) default termination and early exit, including notice periods for the service provider and the Organizations
j) sub-contracting
k) applicable laws of Bangladesh
l) ownership of data
m) fees calculation and conditions
n) start and end date of the agreement where applicable

5.2.7 The contractual agreement shall be vetted by the Organizations‟ legal counsel/Law Department.

5.2.8 The Organization shall ensure that CSP must notify prior to any changes required relevant to the organization.

5.2.9 The Organization shall ensure that CSP has carefully considered the criminal records of its employees.

5.2.10 Service contracts with CSP shall include (but not limited to):

a) Pricing
b) Measurable service/deliverables
c) Timing/schedules
d) Confidentiality clause
e) Contact person names (on daily operations and relationship levels)
f) Roles and responsibilities of contracting parties including an escalation matrix
g) Renewal period
h) Modification clause
i) Frequency of service reporting
j) Termination clause
k) Penalty clause
l) Warranties, including service suppliers‟ employee liabilities, 3rd party liabilities and the related remedies
m) Geographical locations covered
n) Ownership of hardware and software
o) Documentation (e.g., logs of changes, records of reviewing event logs)
p) Right to have information system audit conducted by internal or external audit team or by Bangladesh Bank.

5.2.11 In case of contract termination, data disposal clause 3.6 must be complied.

5.3 Indemnification

5.3.1 The Organization shall clearly define indemnification clause with CSP.

6. Cloud Governance, Risk and Compliance Monitoring

6.1 Roles and Responsibilities

6.1.1 The organization shall ensure shared responsibility and accountability for the services from CSP as per cloud deployment model.

6.1.2 The Organization shall document responsibility matrix.

6.1.3 The Organization shall oversee performance of the CSP and submit the report to the board or an appropriate authority periodically.

6.2 Cloud Governance, Risk and Control

6.2.1 The Organization shall have a cloud security policy in line with this guideline approved by the board.

6.2.2 The Organization shall include following cloud governance and risk mitigation controls in the cloud security policy aligned with business objectives (but not limited to):

a) Data classification
b) Location and jurisdiction
c) Authorization
d) Ownership
e) Custodianship
f) Privacy
g) Contractual control
h) Security control
i) Shared responsibility
j) Risk assessment
k) Incident response
l) Notification
m) Exit process

6.2.3 The Organization shall consider all types of risk sources related to Cloud Computing, including threats and vulnerabilities, which are derived from its features, e.g., networking, scalability and elasticity of the system, resource sharing, self-service provisioning, administration on demand, cross-jurisdictional service provisioning, and limited visibility into the implementation of controls.

6.2.4 The Organization shall document overall risk management process considering cloud specific security and privacy risks.

6.3 Periodic review and Auditing

6.3.1 The Organization shall develop a process for cloud provider assessments internally or by engaging third party at least once a year. This should include but not limited to:

a) Contract review.
b) Self-reported compliance review.
c) Documentation and policies.

d) Available audits and assessments.
e) Service reviews.
f) Change-management policies and change governance.

6.3.2 The Organization shall ensure monitoring, auditing and alerting are configured to capture the changes in the system in real-time.

6.3.3 The Organization shall ensure that there is no vendor lock-in from CSP.

6.3.4 The Organization shall ensure SOC 2 (Service Organization Control 2) Type II audit of CSP.

6.4 Threat, Vulnerability Assessment and Penetration Testing

6.4.1 The Organization shall ensure that the service provider has a formalized process in place to identify, classify and remediate vulnerabilities in its service on an ongoing basis.

6.4.2 The Organization shall conduct a periodic assessment to identify new vulnerabilities, and schedule the patching activities to remediate the vulnerabilities in accordance with their criticality.

6.4.3 The Organization may consult the CSP prior to engaging Penetration Testing to understand any technical limitations of testing and ensure awareness.

6.4.4 The Organization shall define and maintain the standard rules of engagement during Vulnerability Assessment and Penetration Testing (VAPT).

6.4.5 The Organization shall ensure that appropriate mitigation process is identified until remediation.

6.4.6 The Organization shall avoid providing the CSP with account credentials and/or access to systems outside of their responsibility.

6.5 Security Incident Management, e-Discovery, & Cloud Forensics

6.5.1 The Organization shall have a formalized process which should be in place to monitor for and respond to incidents in a timely fashion.

6.5.2 The use of cloud service shall not prevent the Organization from fulfilling its responsibilities in response to a forensic investigation.

6.6 Legal and Regulatory Requirements in Cloud Computing

6.6.1 Adherence to Laws

6.6.1.1 The Organizations are bound by the law of the country wherein they operate.

6.6.2 Service Level Agreement

6.6.2.1 Enforceable and measurable Service Level Agreements (SLAs) shall be in place for outsourcing arrangements.

6.6.3 Standard Certification

6.6.3.1 The Organization shall ensure that the CSP achieves and maintains the ISO/IEC (International Organization for Standardization/International Electrotechnical

Commission) 27017 or CSA START (Cloud Security Alliance the Security, Trust, Assurance, and Risk (STAR) registry).

6.6.3.2 The Organization may ensure that the CSP obtains and maintains ISO 27001 certification.

6.6.3.3 The Organization which wants to provide card services shall ensure that the CSP obtains and maintains PCI DSS certification.

6.6.3.4 The Organization shall ensure that the CSP must comply with ISO22301 and ISO 24762 standards to ensure Business Continuity Plan (BCP)/ Disaster Recovery Plan (DRP).

6.6.3.5 The Organization may ensure that the CSP must comply with ISO 27005 standards.

6.6.4 Compensation for Data Loss/Misuse

6.6.4.1 The Organization shall have arrangement for appropriate compensation for data loss or misuse in the agreement with CSPs.

6.7 Data Security

6.7.1 The Organization shall develop a data security model focusing on data, people and infrastructure. This may include:

a) Authentication
b) Access control
c) Secondary approval
d) User behavior analytics
e) Logging & reporting
f) Data discovery
g) Asset and data classification
h) Encryption
i) Key management
j) Configuration hardening
k) Logical segmentation
l) Boundary enforcement, etc.

6.8 Ownership of Data

6.8.1 The Organization shall ensure that every business data has an owner.

6.8.2 The Organization shall ensure that the CSP has no rights or licenses to use data.

6.8.3 The Organization shall ensure that the CSP does not acquire and shall not claim any security interest in customer data.

6.9 Contractual Requirements for Cloud Service Providers :

The Organization shall include (not limited to)

6.9.1 A detailed description of the service environment, including facility locations and applicable access control requirements

6.9.2 Predefined service levels (i.e. required „up-time" percentage minimums) and associated costs, including non-negotiable taxes, levies, and fees imposed by the provider or any government agency.

6.9.3 Specific remedies for a specific harm caused or resulting from any non-compliant activities by the cloud provider

6.9.4 The period of performance and due dates for any deliverables.

6.9.5 The cloud provider"s points of interface with the Organization.

6.9.6 The Organization"s responsibilities for providing relevant information and resources to the CSP.

6.9.7 Procedures, protections, and restrictions for co-locating or commingling the Organizational data and for handling sensitive data

6.9.8 Procedures dealing with system access and data availability with respect to electronic discovery

6.9.9 The process for assessing the cloud provider"s compliance with the service level agreement, including independent audits and testing

6.9.10 The cloud provider"s obligations upon contract termination, such as the process for returning and/or permanently expunging of the Organizational data.

6.9.11 The Organization shall ensure that the CSP must comply and maintain Non-disclosure agreement (NDA)

6.10 Audit and Compliance

6.10.1 The Organization shall provide unrestricted access to their data and all relevant information for the Organization, to its auditors and Bangladesh Bank.

6.10.2 The Organization shall exercise its access and audit rights, taking a risk-based approach.

6.10.3 The Organization when performing audits in multi-client or multi-tenant environments, they should take care of risks to another client"s environment are avoided or mitigated.

6.10.4 Rights to audit the CSP's compliance with the agreement including rights of access to the CSP's premises where relevant records and data are being stored.

6.10.5 The Organization may appoint an external auditor to perform audit in the CSP"s relevant environments.

6.10.6 The Organization shall ensure proper compliance of all audit findings and recommendations.

7. Education, Training and Awareness

7.1. Training and awareness

Banking on the cloud requires a different skill-set along with a different mindset. With proper cloud training, IT professionals can provide better support in scaling a business. With well-trained employees, Organizations can improve their productivity and take competitive advantage. Additionally, an Organization can ensure a secure environment where they can do their activities more efficiently and cost-effectively.

7.1.1. The Organization shall ensure that all relevant personnel are getting proper training, education, updates and awareness of Cloud Computing activities relevant to their job function in managing products, services, and the systems of the Organization.

7.1.2. The Organization shall arrange basic training/workshop regarding Cloud Computing for all relevant employees.

7.1.3. The Organization shall ensure appropriate skill sets of top management relating to Cloud Computing adaptation and management.

7.1.4. The Organization shall develop a cloud skills development strategy to map the current skills of team members as well as to keep pace with the innovations required to stay at the top of the field.

7.1.5. The Organization shall ensure adequate training/awareness facilities for IS Audit team on the context of Cloud Computing.

7.1.6. The Organization shall ensure relevant professional certification(s) for the officials engaged in cloud computing.