Consultation Paper on Cloud Framework

Version 1.0

Securities and Exchange Board of India
Plot no. C4-A, G Block Bandra Kurla Complex,
Bandra (East), Mumbai – 400051, India
Tel.: +91-22-26449000/40459000
Website: www.sebi.gov.in

This page intentionally left blank

Executive Summary

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 – NIST Definition.

Cloud computing has common characteristics like on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Due to these characteristics, cloud computing has advantages like reduced IT costs, scalability, business continuity, accessibility anywhere, with any device, higher performance and availability, quick application deployment etc. When contemplating cloud adoption, factors including risk identification, control mechanisms, security and operational standards, vendor lock-in and compliance with the legal, technical and regulatory requirements must be taken into account.

The consultation paper is based on the lengthy and exhaustive study, survey, and consultations with market participants (MIIs and brokers), regulators, cloud associations, cloud service providers (CSPs), government agencies, and SEBI Steering Committee. The summary of the framework is as follows:

i. There are no limitations on using any cloud deployment model. The SEBI regulated entity (RE) may adopt for cloud computing depending on their business and technology risk assessment.
ii. It is to be noted that although the IT services/ functionality can be outsourced (to a cloud based solution), RE are solely accountable for all aspects related to the cloud services including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with respect to the laws, rules, regulations, circulars, etc. issued by SEBI/ Union Government/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.
iii. The cloud services should be taken only from the MeitY empaneled cloud service provider's (CSP's) data centers. The CSP's data center should hold a valid STQC (or any other equivalent agency appointed by Government of India) audit status.
iv. In a multi-tenant cloud architecture, adequate controls shall be provisioned to ensure that data (in transit, at rest and in process) shall be isolated and inaccessible to any other tenant. RE shall assess and ensure the multi tenancy segregation controls placed by CSP and place additional security controls if required.
v. Data shall be encrypted at any lifecycle stage (at rest, in transit, in use), source or location to ensure the confidentiality, privacy and integrity.
vi. RE shall retain complete ownership of its data and associated data, encryption keys, logs etc. residing in cloud.

vii. Compliance with legal and regulatory requirements has to be ensured by the RE.
viii. The cloud deployments of RE shall be monitored through in-house Security Operations Centre (SOC), a third-party SOC or a managed SOC.
ix. Necessary provisions for audit and inspection of CSP and its sub-contractor or engage third party auditor to conduct audit and inspection should be included.
x. The agreement between the RE and CSP shall cover security controls, legal and regulatory compliances, clear demarcation of roles, and liabilities, appropriate services and performance standards etc.

The proposed cloud framework will guide RE to adopt cloud computing for augmenting the business prospects by scalability, reduced operational cost, digital transformation and reducing IT infrastructure complexity.

The proposed cloud framework is a principle based framework which has nine suggested high-level principles. This document attempts to address the risks associated with cloud adoption and the necessary mandatory controls. The document suggests baseline security required to be implemented and RE shall decide as per the business and technology risk assessment, and risk appetite of their organization, and as per compliance with all the applicable circulars/ guidelines/ advisories issued by SEBI from time to time.

Table of Contents

Abbreviations:

Sr. No.	Abbreviation	Explanation/Expansion
1	**2FA**	2 Factor Authentication
2	**API**	Application Programming Interface
3	**BCP**	Business Continuity Plan
4	**CISO**	Chief Information Security Officer
5	**CSP**	Cloud Service Provider
6	**DDOS**	Distributed Denial-of-Service
7	**Dev**	Development Environment
8	**HPSC-CS**	High Powered Steering Committee on Cyber Security
9	**IPS**	Intrusion Prevention System
10	**LAN**	Local Area Network
11	**MII**	Market Infrastructure Institution
12	**MPLS**	Multiprotocol Label Switching
13	**MSP**	Managed Service Provider
14	**NIST**	National Institute of Standards and Technology
15	**P2P**	Point-to-Point connection
16	**PII**	Personal Identifiable Information
17	**RE**	Regulated Entity(ies) [includes all market participants, including MIIs, registered with SEBI]
18	**SI**	System Integrator
19	**SOAR**	Security Orchestration, Automation and Response
20	**SOC**	Security Operation Center
21	**SSL**	Secure Sockets Layer
22	**STQC**	Standardization Testing and Quality Certification
23	**UAT**	User Acceptance Testing Environment
24	**VAPT**	Vulnerability Assessment & Penetration Testing
25	**VM**	Virtual Machine
26	**VPN**	Virtual Private Network
27	**WAF**	Web Application Firewall

Definitions

1. Cloud model descriptions-
   The various cloud models and their functional description are given below:

Sr. No	Model	Description
1	Private Cloud	A single tenant environment (i.e. all the resources are utilized/ accessible to only one customer) hosted at on-site location (i.e. location owned by the customer).
2	Hosted Private Cloud	A single tenant environment (i.e. all the resources are utilized/ accessible to only one customer) hosted at an off-site location (i.e. location not owned by the customer) owned by a third-party.
3	Public Cloud	A multi-tenant environment (i.e. resources are being used by multiple customers at the same time) hosted at an off-site location owned by a third-party.

2. Cloud Service Models-
   The definitions of various cloud service models (as per NIST) are given below (the other models such as Application as a Service, Security as a Service, etc. may be considered as a sub-part of the below models):
   i. **Infrastructure as a Service (IaaS)**: The capability provided to the consumer is to provision 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. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

   ii. **Platform as a Service (PaaS)**: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

   iii. **Software as a Service (SaaS)**: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin

client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

A. Background

In the recent times the dependence on cloud solutions for delivering the IT services is increasing. While cloud solutions offer multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., a RE should also be aware of the new cyber security risks and challenges which cloud solutions introduce. In view of the above, a cloud framework has been drafted to address the risks effectively and ensure the legal and regulatory compliance. The proposed framework shall be seen as an addition to already existing SEBI circulars /guidelines /advisories issued time to time.

B. Objective

The major purpose of this framework is to highlights the key risks and control measures which RE need to consider before adopting cloud based solutions. The document also sets out the regulatory and legal expectations from RE if they adopt cloud computing solutions.

C. Applicability

The proposed framework once approved shall come into force with immediate effect for all new cloud onboarding assignments. However REs who are already availing cloud services shall ensure that all such arrangements shall be revised and shall be reassessed in compliance with these directions not later than ……....[stakeholders may suggest what timeline should be given] from the date of issuance of the final approved framework.

D. Study Undertaken and the Observations from the Study

A study was done on MIIs and brokers to understand the current status of deployments in cloud and their adherence with security controls as defined in SEBI cyber security and cyber resilience framework. As part of this study, inputs were also taken from CSPs and industry associations.

On the basis of the above mentioned study, the following may be noted:

i. It was observed that there is no restriction on cloud models by any government bodies across domestic and international jurisdictions. However, approach for cloud adoption should necessarily cover risk identification, control measures, security and operational practices and adherence with the legal, technical and regulatory aspects.

ii. It was also observed that there is a segregation of technical responsibilities (with respect to the various tasks/ functions) between the RE and CSP. However, the accountability with respect to ensuring compliance with laws, rules, regulations, etc. issued by SEBI/ Union government/ respective state government rests completely with the RE.

E. Due Diligence before Adoption of Cloud based Services

It is recommended that before opting for cloud based services, the Board/ Partners/ Owners of the market participants should evaluate the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing. An analysis (including but not limited to comparative analysis, SWOT analysis, etc.) may also be conducted on the type of cloud model to be adopted based on the need, suitability, capability of the organization, etc. The above mentioned evaluation / analysis should be conducted keeping in mind that although the IT services/ functionality can be outsourced (to a cloud based solution), RE are ultimately accountable for all aspects related to the cloud services including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with respect to the laws, rules, regulations, circulars, etc. issued by SEBI/ Union Government/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

F. Approach

The proposed cloud framework is a principle based framework which covers GRC, data localization, data ownership and process visibility, access, risk assessment and due-diligence on CSPs, security controls, legal and regulatory obligations, DR & BCP and vendor lock-in. The principles are drafted as high level, broadly stated guidelines to set the standards by which RE must comply with while adopting cloud deployment models. The principles are stated below:

i. *Principle 1*: Governance, Risk and Compliance Sub-Framework
ii. *Principle 2*: Data Residency and Sovereignty
iii. *Principle 3*: Data Ownership and Visibility in CSPs Infrastructure and Processes
iv. *Principle 4*: Responsibility of the Cloud Solution
v. *Principle 5*: Due Diligence by the RE
vi. *Principle 6*: Security Controls
vii. *Principle 7*: Contractual and Regulatory Obligations
viii. *Principle 8*: BCP, Disaster Recovery & Cyber Resilience
ix. *Principle 9*: Vendor Lock-in and Concentration Risk Management

The following sections detail each of the principles mentioned above.

Principle 1: Governance, Risk and Compliance Sub-Framework

1. Governance, Risk and Compliance (GRC):

RE shall adhere with the governance framework mentioned in various cybersecurity and outsourcing circulars issued by SEBI time to time, in addition to adhering with the following cloud based GRC sub-framework:

i. **Cloud Governance**: The RE shall have a Board/ partners/ proprietor (as the case may be) {hereinafter referred to as "the Board"} approved governance model for cloud computing in place. The model shall include:
   1. Strategies of cloud adoption such as cloud service models, deployment models etc.,
   2. Type of services to be on boarded on cloud considering various factor such as data classification, criticality of operations etc.
   3. Measures to ensure the protection of stakeholder's interests
   4. Complying with legal and regulatory requirements.

ii. **Cloud Risk Management**: There is a paradigm shift in the manner how cloud technology is built and managed in comparison with traditional on–premise infrastructure. Therefore, a separate cloud risk management sub-framework shall be in place which should be approved by the Board. The cloud risk management sub-framework shall provide details regarding the various risks of cloud adoption such as technical, legal, compliance etc., and the commensurate risk mitigation controls which should be proportionate to the criticality and sensitivity of the data/operations to be on-boarded on the cloud. A clearly identified and named resource (typically CISO) shall be appointed and shall be responsible for security of the deployments in cloud. A thorough risk assessment shall be done prior to initiation of the project/work keeping in mind that the RE cannot outsource the risks and decision making associated with deployment of cloud services to the CSP.

iii. **Compliance and Legal Aspects:** RE shall comply with guidelines/circulars/advisories issued by SEBI and agencies of Government of India like MeitY, CERT-In etc. from time to time. Processes shall be in place to ensure compliance with applicable legal and regulatory requirements for deployments in cloud.

iv. In order to ensure the smooth functioning and adherence with this sub-framework it is mandated to divide the roles and assign the responsibilities as given below:
   1. *Role of the Board*- The Board shall be responsible for:

a. Approval and review of cloud governance model and cloud risk management sub-framework and setting up a process for smooth on boarding on cloud while adhering with all legal, regulatory, technical and business objectives.
b. Review of cloud governance model and cloud risk management sub-framework at least once every year.
c. Set up the administrative responsibility of senior management.

2. *Role of Senior Management* - The senior management shall be responsible for:
   a. Preparation and adherence with various policies related to cloud adoption.
   b. Periodic assessment (independent or third party) and mitigation of risks arising out of cloud deployments.
   c. Continually monitoring and responding to the risks and intimate the same to board in a timely manner.
   d. Assessment, at least on an annual basis, to review the financial and operational condition of the CSP to assess its ability to continue to meet the various legal, business, compliance etc. requirements of RE and highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness to board in a timely manner.
   e. Periodic evaluation of the adherence of the cloud engagement with regulatory, legal and business objectives.
   f. Management of Human Resources:
      i. Identification of potential skill gaps which emerge as a result of transition to cloud based services.
      ii. Capacity building within organization to build adequate skillsets to manage cloud deployments effectively.

3. *Role of IT team*- The role of IT team is day to day operations and assisting senior management in achieving the objectives of risk management of cloud deployments.

4. The above mentioned responsibilities are indicative in nature and additional roles/ responsibilities may be added (to the Board, senior management, etc.) as per requirements of the RE.

v. **Grievance Redressal Mechanism**: RE shall have a robust grievance redressal mechanism, which in no way shall be compromised on account of cloud adoption i.e., responsibility and accountability for redressal of investors' grievances related to cloud on boarded services shall rest with the RE. Cloud arrangements shall not

affect the rights of the investor against the RE, including the ability of the investor to obtain redressal as applicable under relevant laws.

vi. **Monitoring and Control of Cloud Deployments**:

1. RE shall have in place a management structure to monitor and control the activities and services deployed on cloud. This shall include but not limited to monitoring the performance, uptime of the systems/ resources, service availability, adherence to SLA requirements, incident response mechanism, etc.

2. RE shall conduct regular audits of the cloud deployments. The frequency and scope of such audits shall be in line with SEBI cyber guidelines/circulars/framework issued time to time. Such periodic audits shall assess the performance of the CSP, adequacy of the risk management practices adopted by the CSP, compliance with laws/regulations etc.

vii. **Country Risk**: The engagement with a CSP provider having country of origin outside of India, exposes the RE to country risk. To manage such risk, the RE shall closely monitor the CSP's country's government policies and its political, social, economic and legal conditions on a continuous basis, and establish sound procedures for mitigating the country risk. This includes, inter alia, having appropriate contingency and exit strategies. Further, it shall be ensured that availability of records to the RE and the supervising authority will not be affected even in case of liquidation of the CSP.

In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified.

.

Principle 2: Data Residency and Sovereignty

2. Data Residency & Sovereignty:

The storage/ processing of data (DC, DR, near DR etc.) including logs and any other data pertaining to RE in any form in cloud should be done as per the following conditions:

i. The data should reside/be processed within the legal boundaries of India.

ii. The data should reside/ be processed within the MeitY empaneled CSPs' data centers holding valid STQC (or any other equivalent agency appointed by Government of India) audit status.

Principle 3: Data Ownership and Visibility in CSPs Infrastructure and Processes

3. Data Ownership and Visibility in CSP's infrastructure and processes:

i. **Data Ownership:** The RE shall retain the complete ownership of its data and associated data, encryption keys, logs etc. residing in cloud. CSP shall be working only in fiduciary capacity.

ii. **Visibility**: The CSP shall provide visibility to RE as well as SEBI into CSP's infrastructure and processes, and shall allow the RE to check the integrity and security of the cloud computing services and compliance to applicable policies and regulations issued by SEBI/ Union government/ respective state government from time to time.

iii. It is to be noted that the RE are ultimately responsible and accountable for security of their data (including logs)/ applications/ services hosted in cloud as well as ensuring compliance with laws, rules, regulations, etc. issued by SEBI/ Union government/ respective state government. Accordingly, RE shall put in place effective mechanism to continuously monitor the CSP /MSP /SI and comply with various regulatory, legal and technical requirements.

iv. Implementation and configuration audit of the resources to be deployed by the RE in cloud environment shall be conducted by the RE itself and the same shall be certified by the RE after closing all non-compliances/ observations before go-live.

Principle 4: Responsibility of the Cloud solution

4. Responsibility and Security:

i. While it is acknowledged that there can be a segregation between the RE and the CSP with respect to (including but not limited to) the infrastructure management, and other technical aspects (for example with respect to data, cybersecurity, management of users, etc.), however, the RE is solely accountable for all aspects related to the cloud service including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with respect to the laws, rules, regulations, circulars, etc. issued by SEBI/ Union Government/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

ii. There shall be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the cloud services between the RE and CSP. There shall be no "shared responsibility" or "joint ownership" for any function/ task/ activity between the RE and CSP. If any function/ task/ activity has to be performed jointly by the RE and CSP, there shall be a clear delineation and fixing of responsibility for each sub-task/ line-item within the task. The aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP.

Principle 5: Due Diligence by the RE

5. Due Diligence with respect to CSPs:

The RE shall conduct its due diligence with respect to CSPs beforehand and on a periodic basis to ensure that legal, regulatory objectives etc. of the RE are not hampered. The due diligence shall be risk based depending on the criticality of the data/ services /operations planned to be on boarded on cloud. The criteria that an RE shall look out for are (including but not limited to):

i. Financial soundness and ability to service commitments even under adverse conditions.

ii. Capability to identify and segregate RE's data.

iii. Security risk assessment, including of the technology assets administered by the CSP.

iv. Ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to establish data ownership.

v. Ability to effectively service all the customers while maintaining confidentiality, especially where a CSP has exposure to multiple entities.

vi. Ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality.

vii. The risks arising out of engaging a third party vendor by CSP shall be assessed by the RE.

viii. RE shall ensure that CSP performs proper screening and background checks of their personnel and outsourcing employees before onboarding into CSP and provides adequate trainings and awareness programs to ensure that the customer services are not hampered due to misconfiguration/inadvertent actions/operational issues/etc.

ix. Capability to comply with the legal requirements, compliance needs, operational aspects, information security, data privacy and reputational risks (in case of incidents) of the RE.

Principle 6: Security Controls

6. Security Controls:

The RE shall ensure its compliance with the circulars (for example cybersecurity circular, systems audit circular, etc.)/ guidelines/ advisories issued by SEBI. Further, in reference to the security controls for adoption of cloud based solution, the following (including but not limited to) are being proposed:

6.1. Security of the Cloud:

RE shall perform the assessment of CSPs to ensure that adequate security controls are in place. Some of the common controls (including but not limited to) that the RE need to check are given below:

i. *Vulnerability Management and Patch Management*: RE shall ensure that CSP has a vulnerability management process in place to mitigate vulnerabilities in all components of the services that the CSP is responsible for. Defined timelines based on the criticality of the vulnerability shall be set by the RE for Vulnerability Management and the same should be agreed upon, and complied with, by the CSP. The RE shall assess and ensure that the patch management of CSP adequately covers the entire infrastructure, applications, etc. The patch management framework shall include the timely patching of all components coming under the purview of CSP.

ii. *Monitoring*: RE shall ensure that CSP has adequate security monitoring solutions in place. The monitoring solutions of CSP shall be responsible for the following:
   1. Monitoring shall cover all components of the cloud. Additionally, the CSP shall continuously monitor the alerts generated and take appropriate actions as per the defined timelines.

   2. The RE shall ensure that any event(s) which may have an impact (financial, reputational, operational, etc.) on the RE shall be intimated to RE by CSP in a timely manner.

iii. *Incident Management*: The RE shall ensure that the CSP has incident management processes in place, to detect, respond and recover from any incident at the earliest. The processes should aim to minimize the impact to the RE.

iv. Wherever key management is being done by CSP for platform level encryption (for example, full disk encryption or VM level encryption), RE shall assess and

ensure that the entire key lifecycle management is being done by CSP in a secure manner.

v. *Secure User Management*: The RE shall ensure role based access and rule based access shall be strictly followed by CSP for its resources and it shall be based on the principle of least privilege. The following may also be ensured:
   1. Administrators and privileged users shall be given only minimal administrative capabilities for a pre-defined time period and in response to specific issues/ needs.

   2. All administrative privileges/ users shall be tracked via a ticket/ request by the CSP, and the same shall be provided to the RE on request. Further, the RE shall also track any additional privilege granted to any user by the CSP.

   3. Access to systems or interfaces that could provide access to the RE's data is only granted if the RE has given explicit time-limited permission for that access (this applies on a case-by-case basis).

   4. The necessary auditing and monitoring of the same shall be done by CSP and any anomalies shall be reported to the RE.

   5. Multi Factor Authentication shall be used for administrator/ privileged accounts.

vi. *Multi-Tenancy*: In a multi-tenant cloud architecture, the RE shall ensure that CSP has taken adequate controls to ensure that the RE's data (in transit, at rest and in process) shall be isolated and inaccessible to any other tenants. RE shall appropriately assess and ensure the multi tenancy segregation controls placed by CSP and place additional security controls if required. Any access by other tenants/unauthorized access by CSP's resources to RE's data shall be considered as an incident/breach and the CSP shall ensure that the incident/breach is immediately notified to the RE and adequate steps are taken to control the same. During such incident/breach, the RE shall ensure that CSP should provide all related forensic data, reports and event logs as required to the RE/SEBI/CERT-In/ Any government agency for further investigation.

vii. The RE shall ensure that the agreement with the CSP contains clause(s) for safe disposal/replacement of parts which contain RE's information. The RE shall ensure that while disposing/replacing the parts (for example disks, back

up cartridges and any other permanent memory devices etc.) the CSP should destruct/erase data permanently before leaving the premises of CSP.

viii. For further assurance, the RE may assess the availability of SOC-2 reporting of CSP.

ix. RE shall ensure that CSP has adequate controls in place to safeguard cloud infrastructure as well as ensure the privacy, confidentiality, availability, processing integrity and security of the RE's data right from data creation/transfer/etc. in the cloud till final expunging of data.

6.2. Security in the Cloud:

RE shall perform risk based assessment and place adequate controls depending on the criticality of the data/services/operations (to be placed in cloud environment) under the purview of RE. Some of the common controls (including but not limited to) that RE shall put in place are:

6.2.1. Vulnerability Management and Patch Management

The RE shall have a well-defined Vulnerability Management policy in place and should strictly adhere with the same. The policy should also address the vulnerability management aspects of the infrastructure /services /etc. managed by RE in the cloud. The cloud infrastructure shall be up to date in terms of patches/OS/version etc. The patch management policy shall cover the infrastructure of cloud and the policy shall mandate timely patch application.

6.2.2. Vulnerability Assessment and Penetration Testing (VAPT)

The VAPT activity undertaken by RE should also cover the infrastructure and applications/services hosted on cloud solution. The VAPT Tactics, Tools and Procedures should be fine-tuned to test and assess the cloud native risks and vulnerabilities. VAPT should also be conducted before commissioning of any new system.

6.2.3. Incident Management and SOC Integration:

i. The RE shall have incident management policy, procedures and processes in place. The RE shall adhere with the same for deployments being done in cloud.

ii. In-house SOC solution of RE shall be integrated with the infrastructure of cloud. The continuous monitoring shall be done in an integrated

manner and the services deployed in cloud should be treated as an extension of the RE's on premise network. Wherever in- house SOC is not available, the RE may opt for managed SOC solutions, however, the SOC shall have complete visibility of information systems of the RE deployed on cloud and should be capable to take SOAR actions across the information systems owned by the RE. Additionally, only logs, meta-data should be shipped to shared SOC. PII/sensitive data should not be shipped to the SOC.

6.2.4. Continuous Monitoring:

Continuous monitoring to be done by the RE to review the technical, legal and regulatory compliance of CSP and take corrective measures wherever necessary.

6.2.5. Secure User Management:

The RE shall ensure that the following Identity, Authentication and Authorization practices are followed by CSP:

i. Principle of least privilege shall be adopted for granting access to any resources for normal and admin/privileged accounts.

ii. The identity and access management solution should give the complete view of the access permissions applied to all resources. The access permissions shall be reviewed regularly in order to remove any unwanted access.

iii. The access logs should be retained and reviewed frequently for any anomalous events.

iv. Time bound access permissions may be adopted wherever feasible.

v. Multi factor authentication shall be adopted for admin accounts.

6.2.6. Security of Interfaces:

Typical interfaces in a cloud deployment are given below:

6.2.6.1. Management interface:

i. This is the interface provided to the RE by CSP to manage the infrastructure on cloud. This interface is also used to manage the account of the RE assigned by CSP.

ii. To mitigate the risks, the interface shall have Two Factor Authentication (2FA). The access may be allowed only through dedicated lease lines for additional security. The access logs and access list to the interface should be strictly monitored. The traffic to and from the interface shall be regulated through firewall, Intrusion prevention system, etc.

6.2.6.2. Internet facing interfaces:

Any interface which is exposed to public at large in internet in the form of a service/API/etc. is considered as internet facing interface. Adequate security controls such as IPS, Firewall, WAF, Anti DDOS, API gateways etc. should be in place and additional controls such as 2FA authentication, SSL VPN solutions should be considered.

6.2.6.3. Interfaces connected between RE's/relevant organizations (Through P2P or LAN/MPLS etc.) and CSP:

Security controls such as IPS, Firewall, WAF, Anti DDOS, etc. shall be in place and additional controls such as IPSEC VPN wherever necessary shall be adopted.

6.2.7. Secure Software Development:

i. RE shall adopt appropriate Secure Software Development Life Cycle (SSDLC) processes, and security shall be an integral part right from the design phase itself.

ii. A new approach shall be developed for dealing with cloud native development concepts such as micro services, APIs, containers, server less architecture etc. The traditional security mechanism of protecting typical web applications might not be relevant for cloud native development concepts.

iii. Best practices such as zero trust principles, fine grained access control mechanism, API Gateways etc. shall be adopted. Implicit accept methods for APIs on basis of IP address, access key etc. shall not be used. The RE shall categorize the APIs into external facing (internet facing), internal-within application (internal to application) and internal-within cloud infrastructure. End to end security of the APIs shall be taken care by the RE as per standard practices and guidelines.

iv. Secure identification, authentication and authorization mechanisms shall be adopted.

6.2.8. Managed Service Provider(MSP) & System Integrator(SI)

i. Wherever MSP and SI are involved in cloud services procurement, a clear demarcation of roles, and liabilities shall be defined in the Agreement/Contract.

ii. As there are new risks introduced in engaging MSP/SI or both, the same shall be assessed, and mitigation shall be done by the RE.

6.2.9. Encryption and Cryptographic Key Management

i. To ensure the confidentiality, privacy and integrity of the data, encryption as defined below shall be adopted by the RE:
   1. Data-at-rest encryption to be done with strong encryption algorithms. Data object encryption, file level encryption or tokenization in addition to the encryption provided at the platform level shall be used.

   2. Data-in-motion including the data within the public cloud shall be encrypted. Session encryption or data object encryption in addition to the encryption provided at the platform level (Ex. TLS encryption) shall be used wherever the sensitive data is in transit.

   3. Data-in-use i.e. wherever data that is being used or processed in the public cloud, confidential computing solutions shall be implemented.

ii. “Bring Your Own Key” approach shall be adopted, which ensures that the RE retains the control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption.

iii. “Bring Your Own Encryption” (BYOE) approach shall be followed by the RE wherever necessary.

iv. Generating, storing and managing the keys in a Hardware Security Module (HSM) shall be implemented in the RE’s premises in order to have control of key generation. However, it is to be noted that HSM should be designed in fault tolerance mode to ensure that the failure of HSM should not have an impact on data retrieval and processing.

6.2.10. End Point Security

The RE shall ensure that the data security controls such as anti-virus, Data Leak Prevention (DLP) solution etc. are installed and configured on the cloud deployments for effective data security.

6.2.11. Network Security

i. RE shall adopt the micro segmentation principle on cloud infrastructure. Only the essential communication channels between computing resources shall be allowed and the rest of the communication channels shall be blocked.
ii. RE may consider the option of employing Cloud Access Security Broker (CASB) and Secure Access Service Edge (SASE) for effective monitoring, enforcement of policies etc.

6.2.12. Backup and recovery solution

i. The RE shall ensure that a backup and recovery policy is in place to address the backup requirement of cloud deployments. The backup and recovery processes shall be checked at least twice in a year to ensure the adequacy of the backups.
ii. The backup shall be logically segregated from production/dev environment to ensure that the malware infection in production systems should not percolate to backup environment.
iii. When CSP's backup services are utilized, adequate care should be taken with encryption solution and key management.

6.2.13. Skillset

Adequate skillset shall be developed in house by RE to manage risks associated with public cloud solutions. The skills should be imparted to oversee the management interfaces, security configurations etc. of CSP infrastructure. This is a critical factor as it will reduce the misconfigurations, vulnerabilities etc. and increase the reliability of services.

6.2.14. Breach Notification

CSP shall notify the RE of any potential breach incident or any actual breach as mandated by the RE. The CSP shall provide all related forensic data, reports and event logs as required by RE/ SEBI/ CERT-In/ Any other government agency. The incident shall be dealt as per the Security Incident Management Policy of the RE along with the relevant guidelines/ directions issued by SEBI/ Union Government/ respective state government.

Principle 7: Contractual and Regulatory Obligations

7. Contractual and Regulatory Obligations

i. The contractual/agreement terms between RE and CSP shall include the provisions for performing audit by the RE, and information access rights to the RE as well as SEBI for the purpose of performing due diligence and carrying out supervisory reviews. RE shall also ensure that their ability to manage risks, provide supervision and comply with regulatory requirements is not hampered by the contractual terms and agreement with CSP.

ii. The contract/agreement shall be vetted with respect to legal and technical standpoint by the RE. The agreement shall be flexible enough to allow the RE to retain adequate control over the resources which are on boarded on cloud and the right to intervene with appropriate measures to meet legal and regulatory obligations.

iii. SEBI/ CERT-In/ Any other government agency/ RE may at any time, with prior notice:

1. Conduct direct audits and inspection of CSP and its sub-contractor or engage third party auditor to conduct the same and check the adherence with SEBI and government guidelines/policies/circulars and industry standard policies.
2. Perform search and seizure of data pertaining to the RE and relevant sources (Ex. hypervisor logs pertaining to the RE's infrastructure etc.). In this process SEBI or SEBI authorized resources may access RE's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the CSP and/ or its sub-contractors.
3. Engage a forensic auditor to identify the root cause of any incident (cyber security or other incidents)
4. Seek the audit reports of the audits conducted by CSP.

The RE shall ensure that adequate provisions are included in the agreement/contract with CSP to enable the above functionalities.

iv. Contract/Agreement should have adequate terms regarding the termination of contract with CSP and appropriate exit strategies which ensure smooth exit without hindering the legal, regulatory, technical etc. obligations of RE.

v. As part of exit strategy, a clear expunging clause shall be defined in agreement with CSP, which shall state that whenever the RE intends to expunge the data, there shall not be any traces of the data in disks, backup devices, logs, etc. and no data shall remain in recoverable form. However, it is the responsibility of the RE to ensure that the minimum retention requirements for data (including logs) as

prescribed by SEBI/ Union government/ respective state government are met and that the required data, logs, etc. are archived, even if the RE moves out of the cloud/ changes CSPs.

vi. The RE shall ensure that their data (including but not limited to logs, business data, etc.) is stored in an easily accessible manner (during utilization of cloud services and after exit from cloud services) and it shall be provided to SEBI/ any other government agency whenever required.

vii. The RE are required to adhere with SEBI circulars issued from time to time and the proposed cloud framework shall be seen as an addition/ complementary to existing guidelines and not as a replacement.

viii. The agreement/contract made by RE shall also include (but not limited to) below mentioned terms:

1. Definition of the IT activity and resources being on boarded on cloud, including appropriate service and performance standards including for the sub-contractors, if any.
2. Effective access to all the objects/ information relevant to the RE/ RE's operation including data, books, records, logs, alerts, and data centre.
3. Continuous monitoring and assessment of the CSP by the RE so that any necessary corrective measure can be taken immediately, including termination of contract and any minimum period required to execute such provision, if deemed necessary.
4. Type of material adverse events (e.g., data breaches, denial of service, service unavailability etc.) and incident reporting requirements to the RE to take prompt mitigation and recovery measures and ensure compliance with statutory and regulatory guidelines.
5. Compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer data.
6. The deliverables, including Service-Level Agreements (SLAs) formalizing the performance criteria to measure the quality and quantity of service levels;
7. Storage of data (as applicable to the RE) only within the legal boundaries of India as per extant regulatory requirements.
8. Clauses requiring the CSP to provide details of data (related to RE and its customers) captured, processed and stored.
9. Controls for maintaining confidentiality of data of RE and its customers, and incorporating CSP's liability to the RE in the event of security breach and leakage of such information.

10. Types of data/ information that the CSP is permitted to share with the RE's customers and/or any other party.
11. Specifying the resolution process for events of default, indemnities, remedies, and recourse available to the respective parties.
12. Contingency plan(s) to ensure business continuity planning and recovery requirements.
13. Right to conduct audit of the CSP by the RE, whether by its internal or external auditors on its behalf, and to obtain copies of any audit or review reports and findings about the CSP with respect to the services performed for the RE.
14. Right to seek information from the CSP about the third parties (in the supply chain) engaged by the CSP.
15. Clauses making the CSP contractually liable for the performance and risk management practices of its sub-contractors.
16. Obligation of the CSP to comply with directions issued by the SEBI in relation to the activities of the RE on boarded on cloud.
17. Termination rights of the RE, including the ability to orderly transfer the proposed cloud onboarding assignment to another CSP, if necessary or desirable.
18. Obligation of the CSP to co-operate with the relevant authorities in case involving the RE as and when required.

ix. Wherever the System integrator or managed service provider or both, along with CSP are involved, the contractual terms and agreement shall unambiguously demarcate/ delineate the roles, and liabilities of each participating party (in-line with the Principle 4: Responsibility of the Cloud Solution of the proposed framework) for each task/ activity/ function. There shall be no "shared responsibility" or "joint ownership" for any task/ activity/ function/ component.

x. If any function/ task/ activity has to be performed jointly by the RE and CSP, there shall be a clear delineation and fixing of responsibility between the RE and the CSP for each sub-task/ line-item within the task. The aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP.

xi. Reporting Requirements:
    1. It is being reiterated that the RE are solely accountable for all aspects related to the cloud services including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with respect to the laws, rules, regulations, circulars, etc. issued by SEBI/ Union Government/ respective state government.

2. As part of system audit conducted by the RE, the auditor shall verify whether there is a clear delineation/ demarcation of roles and responsibilities for each task/ function/ activity/ component between the RE and the CSP (as provided in ix and x above), and the same has been incorporated in the agreement/ contract signed between the RE and CSP. The auditor shall also verify whether the demarcation of the responsibilities has been implemented in-line with the agreement.
3. The RE shall also explicitly and unambiguously specify the party (RE or CSP) which is responsible for ensuring compliance with each clause of the SEBI circulars (for example cybersecurity circular, systems audit, etc.) in their statutory audit report. There shall be no “shared responsibility” or “joint ownership” for any of the clauses. In case the responsibility of ensuring compliance (for any clause) rests with both parties, the task shall be split into sub-tasks/line-items, and for each sub-task/line-items, the responsible party shall be indicated in the report.
4. The RE shall ensure that the demarcation/ delineation of responsibilities is provided for each clause of the circular(s).
5. As part of the audit report, the RE shall also include the auditor’s certification that the delineation/ demarcation for every task/ activity/ function/ component has been stated (in the agreement) and implemented by the RE. Additionally, compliance with respect to the proposed cloud framework shall also be submitted along with the audit report.

Principle 8: BCP, Disaster Recovery & Cyber Resilience

8. Business Continuity Planning (BCP), Disaster Recovery & Cyber Resilience

i. The RE shall assess their BCP framework and ensure that it is in compliance with proposed cloud framework as well as other guidelines/ circulars issued by SEBI.

ii. RE shall also assess the capabilities of preparedness and readiness for cyber resilience of CSP. The same can be periodically assessed by conducting DR drills (in accordance with SEBI circulars issued from time to time) by involving necessary stakeholders.

Principle 9: Vendor Lock-In and Concentration Risk Management

9. Concentration Risk Management

i. RE shall assess their exposure to CSP lock-in and concentration risks. The risk evaluation shall be done before entering into contract/ agreement with CSP and the same should be assessed on a periodic basis.

ii. In order to mitigate the CSP concentration risks, RE shall work on cloud-ready and CSP agnostic solutions (such as implementing a multi-cloud ready solutions) which can facilitate the RE in migrating the solutions as and when necessary with minimal changes. Exit strategies should be developed, which shall consider the pertinent risk indicators, exit triggers, exit scenarios, portability of the data and possible migration options, etc.

iii. The RE should also monitor for the concentration risk arising out of onboarding on a single CSP by multiple RE including itself.

10. Recommendations:

i. RE are solely accountable for all aspects related to their cloud services including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with respect to the laws, rules, regulations, circulars, etc. issued by SEBI/ Union Government/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

ii. There should be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (technical, managerial, governance related, etc.) of the cloud services between the RE and CSP. There shall be no "shared responsibility" or "joint ownership" for any function/ task/ activity between the RE and CSP. If any function/ task/ activity has to be performed jointly by the RE and CSP, there should be a clear delineation and fixing of responsibility between the RE and the CSP for each sub-task/ line-item within the task. The same should be a part of the agreement (as an annexure) between the RE and the CSP.

iii. As part of system audit conducted by the RE, the auditor should verify whether there is a clear delineation/ demarcation of roles and responsibilities for each task/ function/ activity/ component between the RE and the CSP, and the same has been incorporated in the agreement/ contract signed between the RE and CSP. The auditor should also verify whether the demarcation of the responsibilities has been implemented in-line with the agreement and submit the same as part of statutory audit report of the RE.

iv. The cloud services should be taken only from the MeitY empaneled CSPs. The CSP's data center should hold a valid STQC (or any other equivalent agency appointed by Government of India) audit status.

v. RE may opt for any model of deployment on the basis of business and technology risk assessment. However, there should be deployment of commensurate security controls, and compliance should be ensured with rules/ laws/ regulations made by SEBI/ Union government/ respective state government.

vi. The proposed cloud framework should be read along with the circulars (including circulars on outsourcing), directions, etc. issued by SEBI from time to time.

11. List of References:

The below given documents, inter alia, have been referred while preparing the SEBI public cloud adoption policy:

i. *Singapore MAS advisory on addressing the technology and cyber security risks associated with public cloud adoption*
ii. *Whitepaper released by DSCI as an input to the Ministry of Electronics and Information Technology's (MeitY)*
iii. *Cloud security guidance issued by National Cyber Security Center of UK*
iv. *RBI's draft Master Direction on Outsourcing of IT Services*
v. *Appendix of RMIT: Cloud Technology Risk Assessment Guideline (CTRAG) by bank Negara Malaysia*
vi. *Federal Cloud Computing Strategy (USA)*
vii. *Principles on Outsourcing (International Organization of Securities Commissions)*
viii. *Secure Cloud Strategy (Australian Government)*
ix. *Guidance on Cyber Resilience (Reserve Bank of New Zealand)*
x. *Cloud Code of Conduct (European Union)*

12. Any other Suggestions/comments/feedback regarding the cloud framework

i. Considering the implications of the framework on RE, public comments are invited on the proposed cloud framework. The comments/suggestions may be provided as per the format given below:

Name of the person/entity proposing comments:				
Name of the organization (if applicable):				
Contact details:				
Category: whether SEBI regulated entity/CSP/Individual etc.				
Sr. No.	**Extract from Consultation Paper (with details of page no., section no, and clause)**	**Issues**	**Proposals/ Suggestions/ Changes**	**Rationale/ Context/ Remarks**

ii. Comments, as per the aforementioned format, may be sent to SEBI by November 14, 2022 through any of the following modes:
1. By email to: *cloud_framework@sebi.gov.in*
2. By post to the following address:

Ms. Shweta Banerjee (DGM-ITD)
SEBI Bhavan II BKC,
Plot no. C-7, 'G' Block, Bandra Kurla Complex,
Bandra (E), Mumbai (Maharashtra)- 400051

Issued on: November 04, 2022