NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to all members of the Exchange
Circular No. : NCDEX/RISK-003/2023
Date : March 10, 2023
Subject : Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

This is with reference to the SEBI circular no. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023, on the subject **"Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)"**. A copy of the said SEBI circular is enclosed as **Annexure A** for reference.

Members are requested to take note of the contents of the circular and comply.

For and on behalf of
National Commodity & Derivatives Exchange Limited

Sanjay Jain
Senior Vice President and CISO – Enterprise Risk and Governance

For further information / clarifications, please contact
1. Customer Service Group on toll free number: 1800 26 62339
2. Customer Service Group by e-mail to : askus@ncdex.com

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 *March 06, 2023*

प्रति / To,

सभी स्टॉक एक्सचेंज / All Stock Exchanges
सभी समाशोधन निगम (क्लीयरिंग कारपोरेशन) / All Clearing Corporations
सभी निक्षेपागार (डिपॉज़िटरी) / All Depositories
सभी स्टॉक दलाल - एक्सचेंजों के जरिए / All Stock Brokers through Exchanges
सभी निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) - निक्षेपागारों (डिपॉज़िटरी) के जरिए / All Depository Participants through Depositories
सभी म्यूचुअल फंड / आस्ति प्रबंध कंपनियाँ (असेट मैनेजमेंट कंपनी) / न्यासी (ट्रस्टी) कंपनियाँ / म्यूचुअल फंडों के न्यासी मंडल / एएमएफआई / All Mutual Funds / Asset Management Companies / Trustee Companies / Boards of Trustees of Mutual Funds / Association of Mutual Funds in India (AMFI)
सभी केवाईसी रजिस्ट्रीकरण एजेंसियाँ / All KYC Registration Agencies
सभी अर्हित निर्गम रजिस्ट्रार (रजिस्ट्रार टू एन इश्यू) / शेयर अंतरण अभिकर्ता (शेयर ट्रांसफर एजेंट) / All Qualified Registrars to an Issue / Share Transfer Agents

महोदय / महोदया,
Dear Sir / Madam,

विषयः सेबी से विनियमित (रेग्यूलेटेड) एंटिटियों द्वारा क्लाउड संबंधी सेवाएं अपनाने से संबंधित ढाँचा
Sub: Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

1. **पृष्ठभूमि:** पिछले कुछ समय से यह देखने में आया है कि सूचना प्रौद्योगिकी (आईटी) से संबंधित सेवाएं प्रदान करने के लिए क्लाउड कम्प्यूटिंग पर निर्भरता बढ़ती जा रही है । क्लाउड कम्प्यूटिंग के कई फायदे तो हैं ही (जैसे कि सुविधाओं को आसानी से घटाया-बढ़ाया जा सकता है, आसानी से अमल में लाया जा सकता है, अलग से सिस्टम आदि खरीदने पर कोई भी खर्च करने की जरूरत नहीं होती), किंतु इसके साथ-साथ विनियमित (रेग्यूलेटेड) एंटिटियों को यह भी पता होना चाहिए कि क्लाउड कम्प्यूटिंग

1. **Background:** In recent times, the dependence on cloud computing for delivering the IT services is increasing. While cloud computing offers multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., the RE should also be aware of the new cyber security risks and challenges which cloud computing introduces. In view

भी साइबर हमलों से अछूता नहीं रहा है और इसमें भी नई-नई चुनौतियाँ सामने आ रही हैं । इसके मद्देनज़र ही यह ढाँचा तैयार किया गया है, जिसमें विनियमित (रेग्यूलेटेड) एंटिटियों को सुरक्षा के लिहाज से मूलभूत दिशानिर्देश दिए गए हैं, और उन्हें यह भी बताया गया है कि उन्हें किन-किन कानूनी और विनियामक (रेग्यूलेटरी) प्रावधानों का पालन करना होगा । इस ढांचे के साथ-साथ सेबी द्वारा पहले से जारी किए गए परिपत्रों (सर्कुलर) / दिशानिर्देशों (गाइडलाइन्स) / एडवाइज़री का पालन तो करना ही होगा ।

of the above, this cloud framework has been drafted to provide baseline standards of security and for the legal and regulatory compliances by the RE. The framework shall be seen as an addition to already existing SEBI circulars /guidelines /advisories.

2. उद्देश्य: इस ढांचे का मुख्य उद्देश्य यह स्पष्ट करना है कि क्लाउड कम्प्यूटिंग अपनाने में क्या-क्या बड़े जोखिम हो सकते हैं, और इसके लिए विनियमित (रेग्यूलेटेड) एंटिटियों को लाज़िमी तौर पर पहले से ही क्या-क्या कदम उठाने होंगे । इस दस्तावेज में यह भी बताया गया है कि यदि विनियमित (रेग्यूलेटेड) एंटिटियों द्वारा ऐसे सॉल्यूशन अपनाए जाते हैं, तो उन्हें किन-किन विनियामक (रेग्यूलेटरी) और कानूनी प्रावधानों का पालन करना होगा ।

2. Objective: The major purpose of this framework is to highlight the key risks, and mandatory control measures which REs need to put in place before adopting cloud computing. The document also sets out the regulatory and legal compliances by REs if they adopt such solutions.

3. यह ढाँचा :

इन विनियमित (रेग्यूलेटेड) एंटिटियों पर लागू होगा:

i. स्टॉक एक्सचेंज
ii. समाशोधन निगम (क्लीयरिंग कारपोरेशन)
iii. निक्षेपागार (डिपॉज़िटरी)

3. Applicability:

The framework shall be applicable to the following REs:

i. Stock Exchanges
ii. Clearing Corporations
iii. Depositories
iv. Stock Brokers through Exchanges

iv. स्टॉक दलाल - एक्सचेंजों के जरिए

v. निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) - निक्षेपागारों (डिपॉज़िटरी) के जरिए

vi. आस्ति प्रबंध कंपनियाँ (असेट मैनेजमेंट कंपनी / एएमसी) / म्यूचुअल फंड

vii. अर्हित निर्गम रजिस्ट्रार (रजिस्ट्रार टू एन इश्यू) और शेयर अंतरण अभिकर्ता (शेयर ट्रांसफर एजेंट)

viii. केवाईसी रजिस्ट्रीकरण एजेंसियाँ

v. Depository Participants through Depositories

vi. Asset Management Companies (AMCs)/ Mutual Funds (MFs)

vii. Qualified Registrars to an Issue and Share Transfer Agents

viii. KYC Registration Agencies (KRAs)

4. कब व कैसे लागू होगा और कब-कब क्या-क्या जानकारी आदि देनी है

i. यह ढाँचा विनियमित (रेग्यूलेटेड) एंटिटियों के सभी नए या प्रस्तावित क्लाउड प्रोजेक्ट आदि के लिए तुरंत प्रभाव से लागू होगा ।

ii. जो विनियमित (रेग्यूलेटेड) एंटिटियाँ पहले से ही क्लाउड संबंधी सेवाएँ ले रही हैं (यह ढांचा जारी किए जाने की तारीख तक की स्थिति के अनुसार), उन्हें यह सुनिश्चित करना होगा कि जहाँ कहीं भी जरूरी हो, वहाँ इस प्रकार पहले से की गई इन व्यवस्थाओं को इस ढांचे के अनुरूप ढाल लिया जाए और वे [विनियमित (रेग्यूलेटेड) एंटिटियाँ] यह ढांचा लागू होने की तारीख से 12 (बारह) महीनों के भीतर इस ढांचे के प्रावधानों का पालन कर लें ।

4. Transition Period

i. The framework shall come into force with immediate effect for all new or proposed cloud onboarding assignments/ projects of the REs.

ii. REs which are currently availing cloud services (as on date of issuance of this framework) shall ensure that, wherever applicable, all such arrangements are revised and they (RE) shall be in compliance with this framework not later than 12 (twelve) months from the date of issuance of the framework.

iii. इसके अलावा, जो विनियमित (रेग्यूलेटेड) एंटिटियाँ पहले से ही क्लाउड संबंधी सेवाएँ ले रही हैं, उन्हें नीचे दी गई समय-सीमाओं के अनुसार जानकारी / रिपोर्टें प्रस्तुत करनी होंगी :

iii. Additionally, the REs which are currently availing cloud services, shall provide milestone-based updates as follows:

क्र.सं. SN.	समय-सीमा Timeline	जानकारी / रिपोर्ट Milestone
1	इस ढांचे के लागू होने की तारीख से एक (1) महीने के भीतर Within one (1) month of issuance of framework	यदि विनियमित (रेग्यूलेटेड) एंटिटियों के यहाँ पहले से ही कोई क्लाउड संबंधी सेवाएं ली जा रही हों, तो उन्हें उसके ब्यौरे[1] देने होंगे । REs shall provide [1]details of the cloud services, if any, currently deployed by them.
2	इस ढांचे के लागू होने की तारीख से तीन (3) महीनों के भीतर Within three (3) months of issuance of framework	विनियमित (रेग्यूलेटेड) एंटिटियों को एक खाका प्रस्तुत करना होगा कि वे इस ढाँचे को कैसे अमल में लाएँगीं, और इस खाके में उन्हें प्रमुख गतिविधियों, समय-सीमाओं, आदि के ब्यौरे देने होंगे । The REs shall submit a roadmap (including details of major activities, timelines, etc.) for the implementation of the framework.
3	तीन (3) महीनों से बारह (12) महीनों के बीच From three (3) to twelve (12) months of issuance of framework	विनियमित (रेग्यूलेटेड) एंटिटी द्वारा प्रस्तुत किए गए खाके के अनुसार तिमाही प्रगति रिपोर्ट प्रस्तुत की जाएगी । Quarterly progress report as per the roadmap submitted by the RE.

[1] क्लाउड संबंधी सेवाओं के ब्यौरे संलग्नक-क में दिए हुए फॉर्मेट में प्रस्तुत किए जाएँगे ।
The details of cloud deployment shall be submitted in the format provided in Appendix-A

4	इस ढांचे के लागू होने की तारीख से बारह (12) महीनों के बाद After twelve (12) months of issuance of framework	इस ढांचे के प्रावधानों के पालन की रिपोर्ट नियमित रूप से प्रस्तुत की जाएगी । Compliance with respect to the framework to be reported regularly

iv. उपरोक्त जानकारी / रिपोर्टें संबंधित प्राधिकरण को सिस्टम ऑडिट / साइबर सुरक्षा ऑडिट से संबंधित रिपोर्टें प्रस्तुत करने की मौजूदा व्यवस्था के अनुसार प्रस्तुत की जाएंगी ।

iv. The above-mentioned reporting shall be done to the authority as per the existing mechanism of reporting for systems audit/ cybersecurity audit.

5. दायरा :

i. एनआईएसटी के अनुसार, क्लाउड कम्प्यूटिंग में चार तरह के मॉडल होते हैं, यानि कि पब्लिक क्लाउड, कम्यूनिटी क्लाउड, प्राइवेट क्लाउड और हाइब्रिड क्लाउड -

क. यह ढाँचा पब्लिक क्लाउड और कम्यूनिटी क्लाउड को अपनाए जाने के संबंध में लागू है । तदनुसार, यदि विनियमित (रेग्यूलेटेड) एंटिटियाँ इस ढाँचे के तहत निर्धारित की गई शर्तों आदि को पूरा करती हैं, तो वे पब्लिक क्लाउड और कम्यूनिटी क्लाउड की व्यवस्था कर सकती हैं ।

ख. प्राइवेट क्लाउड की व्यवस्था तो आंतरिक स्तर पर अपने लिए ही की जाती है और इसीलिए उन पर सेबी द्वारा समय-समय पर जारी किए गए परिपत्र (सर्कुलर) [जैसे कि साइबर सुरक्षा से संबंधित परिपत्र,

5. Scope:

i. As per NIST, cloud computing has four types of deployment models viz public cloud, community cloud, private cloud and hybrid cloud-

a. This cloud framework is applicable for adoption of public cloud and community cloud. Consequently, REs are permitted to deploy public cloud and community cloud models, subject to the conditions specified herein.

b. A private cloud shall be considered as an on-premise deployment model and consequently, private cloud deployments shall be governed

आउटसोर्सिंग से संबंधित परिपत्र, बीसीपी-डीआर आदि] दिशानिर्देश, एडवाइज़री, आदि लागू होंगे। इस तरह से, विनियमित एंटिटियाँ प्राइवेट क्लाउड की व्यवस्था कर तो सकती हैं, लेकिन इन पर यह ढाँचा लागू नहीं होगा।

by SEBI circulars (for example cybersecurity circular, outsourcing circular, BCP-DR, etc.), guidelines, advisories, etc. issued from time to time. Therefore, private cloud deployments (by REs) are permitted, however, such deployments may not be governed by this cloud framework.

ग. हाइब्रिड क्लाउड तो पब्लिक क्लाउड, कम्यूनिटी क्लाउड और प्राइवेट क्लाउड में से या तो किन्हीं दो का या फिर तीनों का मिला-जुला रूप होता है । इसीलिए, हाइब्रिड क्लाउड के संबंध में तो यह ढाँचा भी लागू होगा और साथ ही साथ सेबी द्वारा जारी किए गए संबंधित परिपत्र (सर्कुलर) / दिशानिर्देश / एडवाइज़री भी लागू होंगे । तदनुसार, यदि इस ढाँचे के तहत निर्धारित की गई शर्तों आदि को पूरा किया जाता है, तो हाइब्रिड क्लाउड की व्यवस्था की जा सकती है ।

c. A hybrid cloud is a combination of two or more out of public cloud, community cloud and private cloud. Therefore, this cloud framework as well as the relevant SEBI circulars/ guidelines/ advisories shall be applicable for hybrid cloud deployments. In view of the above, hybrid cloud deployment is permitted, subject to the conditions specified herein.

ii. इसके अलावा किसी भी दूसरे क्लाउड मॉडल की व्यवस्था तब तक नहीं की जा सकती, जब तक कि इस ढाँचे के तहत स्पष्ट रूप से उल्लेख करके उसकी अनुमति न दे दी जाए । हालांकि, क्लाउड कम्प्यूटिंग एक ऐसी तकनीक

ii. Deployment of any other cloud model is prohibited unless explicitly permitted under this framework. However, as the field of cloud computing is a dynamic and

है जिसमें कुछ न कुछ नयापन आता जा रहा है, इसीलिए सेबी पूरी तरह से विचार-विमर्श करने के बाद ही कुछ और मॉडल की अनुमति दे सकता है, जिसकी जानकारी समय-समय पर सेबी द्वारा दी जा सकती है ।

emerging area, SEBI may allow deployment of other models after due consultations. The same may be specified by SEBI from time to time.

6. आधार :

यह ढाँचा सिद्धांतों के आधार पर निर्धारित किया गया है, जिनमें शामिल हैं - संचालन (गवर्नेंस), जोखिम और पालन (जीआरसी), क्लाउड सेवा प्रदाताओं (सीएसपी) का चयन, डाटा किसका है (डाटा ओनरशिप) और डाटा कहाँ रखा जाना चाहिए (डाटा लोकलाइजेशन), विनियमित एंटिटियों द्वारा पूरी तत्परता बरती जानी, सुरक्षा नियंत्रण (सिक्यूरिटी कंट्रोल), कानूनी और विनियामक बाध्यताएँ, डीआर एवं बीसीपी, और वेंडर लॉक-इन रिस्क । इन सिद्धांतो में मुख्य-मुख्य दिशानिर्देश शामिल किए गए हैं, ताकि विनियमित एंटिटियाँ क्लाउड संबंधी सेवाएं लेते समय इस प्रकार निर्धारित किए गए मानदंडों का पालन करें। ये सिद्धांत इस प्रकार हैं :

i. *सिद्धाँत-1* : संचालन (गवर्नेंस), जोखिम और पालन संबधी उप-ढाँचा
ii. *सिद्धाँत-2* : क्लाउड सेवा प्रदाताओं (सीएसपी) का चयन
iii. *सिद्धाँत-3* : डाटा किसका है (डाटा ओनरशिप) और डाटा कहाँ रखा जाना चाहिए (डाटा लोकलाइजेशन)

6. Approach:

The cloud framework is a principle-based framework which covers Governance, Risk and Compliance (GRC), selection of Cloud Service Providers (CSPs), data ownership and data localization, due- diligence by REs, security controls, legal and regulatory obligations, DR & BCP, and vendor lock-in risk. The principles are broadly stated guidelines to set the standards by which RE must comply with while adopting cloud services. The principles are stated below:

i. *Principle 1*: Governance, Risk and Compliance Sub-Framework
ii. *Principle 2*: Selection of Cloud Service Providers
iii. *Principle 3*: Data Ownership and Data Localization

iv. *सिद्धाँत-4* : विनियमित (रेग्यूलेटेड) एंटिटी की जिम्मेदारी

v. *सिद्धाँत-5* : विनियमित एंटिटी द्वारा पूरी तत्परता बरती जानी

vi. *सिद्धाँत-6* : सुरक्षा नियंत्रण

vii. *सिद्धाँत-7* : कॉण्ट्रैक्ट के अनुसार बाध्यताएँ और विनियामक बाध्यताएँ

viii. *सिद्धाँत-8* : बीसीपी, संकट निवारण (डिज़ास्टर रिकवरी) और साइबर आघात सहने की क्षमता (साइबर रिज़िलियन्स)

ix. *सिद्धाँत-9* : वेंडर लॉक-इन और कन्सेन्ट्रेशन रिस्क मैनेजमेंट

विस्तृत ढाँचा इस परिपत्र (सर्कुलर) के साथ *संलग्नक-1* के रूप में संलग्न है ।

7. यह परिपत्र (सर्कुलर) प्रतिभूतियों (सिक्यूरिटीज़) में निवेश करने वाले निवेशकों के हितों का संरक्षण करने, प्रतिभूति बाजार (सिक्यूरिटीज़ मार्केट) के विकास को बढ़ावा देने तथा उसे विनियमित (रेग्यूलेट) करने के उद्देश्य से, भारतीय प्रतिभूति और विनिमय बोर्ड अधिनियम, 1992 की धारा 11(1) के तहत प्रदान की गई शक्तियों का प्रयोग करते हुए जारी किया जा रहा है ।

iv. *Principle 4*: Responsibility of the Regulated Entity

v. *Principle 5*: Due Diligence by the Regulated Entity

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 detailed framework is enclosed at *Annexure-1* of this circular.

7. This circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

भवदीय / Yours Faithfully,
श्वेता बनर्जी Shweta Banerjee
उप महाप्रबंधक Deputy General Manager
दूरभाष / Phone: 022-26449509
ईमेल / Email: shwetas@sebi.gov.in

Annexure-1

Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

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 and 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 framework is based on the study, survey, and consultations done with market participants, regulators, cloud associations, cloud service providers (CSPs), government agencies, and SEBI Advisory Committees. The summary of the framework is as follows:

i. The RE may opt for any model of deployment on the basis of its business needs and technology risk assessment. However, compliance should be ensured with this cloud framework as well as other rules/ laws/ regulations/ circulars made by SEBI/ Government of India/ respective state government.
ii. It is to be noted that although the IT services/ functionality may be outsourced (to a CSP), RE is solely accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with the laws, rules, regulations, circulars, etc. issued by SEBI/

Government of India/ respective state government. Accordingly, the RE shall be responsible and accountable for any violation of the same.

iii. The cloud services shall be taken only from the Ministry of Electronics and Information Technology (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. For selection of CSPs offering PaaS and SaaS services in India, RE shall choose only such CSPs which:

1. Utilize the underlying infrastructure of MeitY empaneled CSPs for providing services to the RE.
2. Host the application/ platform/ services provided to RE as well as store/ process data of the RE, only within the data centers as empaneled by MeitY and holding 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 motion, at rest and in use) shall be isolated and inaccessible to any other tenant. RE shall assess and ensure that the multi tenancy segregation controls are placed by CSP, and shall place additional security controls if required.

v. Data shall be encrypted at all lifecycle stages (at rest, in motion and in use), source or location to ensure the confidentiality, privacy and integrity.

vi. RE shall retain complete ownership of all its data, encryption keys, logs etc. residing in cloud.

vii. Compliance with legal and regulatory requirements, including the requirements provided in this framework, has to be ensured by the RE at all times.

viii. The cloud deployments of RE shall be monitored through Security Operations Centre (SOC) [in-house, third-party SOC or a managed SOC].

ix. 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.

x. The reporting of compliance (with this framework) shall be done by the REs in their systems audit, cybersecurity audit and VAPT reports, and it shall be done in the standardized format notified by SEBI from time to time

The cloud framework provides mandatory requirements to be fulfilled by the RE for adopting cloud computing to augment the business prospects through scalability, reduced operational cost, digital transformation and reduced IT infrastructure complexity.

The cloud framework is a principle-based framework which has nine high-level principles. The framework highlights the risks associated with cloud adoption and recommends the necessary mandatory controls. The document also recommends baseline security measures required to be implemented (by RE and CSP), and RE may decide to add additional measures as per its business needs, technology risk assessment, risk appetite, compliance requirements in all the applicable circulars/ guidelines/ advisories issued by SEBI from time to time, etc.

Table of Contents

Abbreviations: 13
Definitions 14
1. Governance, Risk and Compliance (GRC): 17
2. Selection of CSPs: 21
3. Data Ownership and Localization: 22
4. Responsibility of the RE (with respect to CSPs): 23
5. Due Diligence by the RE (with respect to CSPs): 25
6. Security Controls: 27
6.1. Security of the Cloud: 27
6.2. Security in the Cloud: 31
6.2.1. Vulnerability Management and Patch Management: 31
6.2.2. Vulnerability Assessment and Penetration Testing (VAPT): 31
6.2.3. Incident Management and SOC Integration: 31
6.2.4. Continuous Monitoring: 32
6.2.5. Secure User Management: 32
6.2.6. Security of Interfaces: 32
6.2.6.1. Management interface: 33
6.2.6.2. Internet facing interfaces: 33
6.2.6.3. Interfaces connected between RE's/relevant organizations (Through P2P or LAN/MPLS etc.) and CSP: 33
6.2.7. Secure Software Development: 33
6.2.8. Managed Service Provider (MSP) & System Integrator (SI): 34
6.2.9. Encryption and Cryptographic Key Management: 34
6.2.10. End Point Security: 36
6.2.11. Network Security: 36
6.2.12. Backup and recovery solution: 36
6.2.13. Skillset: 36
6.2.14. Breach Notification: 37
7. Contractual and Regulatory Obligations: 38
8. Business Continuity Planning (BCP), Disaster Recovery & Cyber Resilience 45
9. Concentration Risk Management 46
10. Recommendations: 47
Appendix-A 52
Appendix-B 53

Abbreviations:

Sr. No.	Abbreviation	Explanation/Expansion
1	2FA	2 Factor Authentication
2	API	Application Programming Interface
3	BCP	Business Continuity Planning
4	CISO	Chief Information Security Officer
5	CSP	Cloud Service Provider
6	DDOS	Distributed Denial-of-Service
7	Dev	Development Environment
8	DR	Disaster Recovery
9	IPS	Intrusion Prevention System
10	LAN	Local Area Network
11	MeitY	Ministry of Electronics and Information Technology
12	MII	Market Infrastructure Institution
13	MPLS	Multiprotocol Label Switching
14	MSP	Managed Service Provider
15	NIST	National Institute of Standards and Technology
16	P2P	Point-to-Point connection
17	PII	Personal Identifiable Information
18	RE	Regulated Entity
19	SI	System Integrator
20	SLA	Service Level Agreement
21	SOAR	Security Orchestration, Automation and Response
22	SOC	Security Operations Center
23	SSL	Secure Sockets Layer
24	STQC	Standardization Testing and Quality Certification
25	UAT	User Acceptance Testing
26	VAPT	Vulnerability Assessment & Penetration Testing
27	VM	Virtual Machine
28	VPN	Virtual Private Network
29	WAF	Web Application Firewall

Definitions

1. *Cloud Model Description-*

   The description of common cloud deployment models (as per NIST)[2] is given below:

Sr. No	Model	Description
1	Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2	Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations 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 organizations in the community, a third party, or some combination of them, and it may exist on or off premises
3	Public Cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider
4	Hybrid Cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

[2] Ref: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

2. *Cloud Service Models-*

A. The definitions of various cloud service models (as per NIST)[3] are given below:

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 software, which can include operating systems and applications. The consumer does not directly 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). A few examples of IaaS are Amazon Web Services (AWS) Elastic Compute Cloud, Microsoft Azure, etc.

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 directly 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. A few examples of PaaS are Google App Engine, Amazon Web Services (AWS) Elastic Beanstalk, etc.

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

[3] Ref: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

configuration settings. A few examples of SaaS are Gmail, Microsoft Office 365, etc.

B. Other deployment models such as Application as a Service, Security as a Service, etc. may be considered as a sub-part or variant of the above-mentioned models as they contain components of IaaS, PaaS and SaaS. For example, Security as a Service is a form of SaaS which provides specialized information security services. Similarly, Application as a Service is a type of SaaS in which applications (for example Google sheets, Google docs, etc.) are delivered on-demand to customers through the internet.

3. *Regulated Entity (RE) –*

   The term "Regulated Entity" refers to SEBI registered/ recognized intermediaries (for example brokers, mutual funds, KYC Registration Agencies, and QRTAs) and Market Infrastructure Institutions (Stock Exchanges, Clearing Corporations, and Depositories) regulated by SEBI.

4. *Key Management-*

   In the context of encryption/ decryption, a key is typically a random string of bits generated to hide (encrypt) or reveal (decrypt) data. A key is most commonly used along with an algorithm (method) for encryption/ decryption of data.

   Therefore, Key management refers to management of cryptographic keys in a system, including their (keys') generation, exchange, storage, etc.

5. *Hardware Security Module (HSM)-*

   A Hardware Security Module is a device that is used for management of Keys, as well as for implementing various functions like encryption, decryption, authentication, etc.

Principle 1: Governance, Risk and Compliance Sub-Framework

1. Governance, Risk and Compliance (GRC):

The REs shall put in place an effective GRC sub-framework for cloud computing to enable them to formulate a cloud strategy suitable for their circumstances/ needs. The RE shall also adhere with the governance framework mentioned in various circulars issued by SEBI. The various aspects that shall be considered by RE (including but not limited to) while formulating the GRC sub-framework are as follows:

i. **Cloud Governance**: The RE shall have a Board/ partners/ proprietors (as the case may be) {hereinafter referred to as "the Board"} approved governance model/ strategy for cloud computing in place. The model/ strategy shall include:
   1. Details of cloud adoption such as cloud service models, deployment models etc.
   2. Type of services to be on boarded on cloud considering various factors such as data classification, criticality of operations, etc. The classification/ categorization shall be done in-line with the circulars/ guidelines issued by SEBI.
   3. Measures to ensure the protection of stakeholder's interests
   4. Measures to comply with the applicable legal and regulatory requirements.

ii. **Cloud Risk Management**:
   1. There is a paradigm shift in the manner of how cloud technology is built and managed in comparison with traditional on–premise infrastructure. Therefore, a comprehensive risk management should be undertaken by the RE to continually identify, monitor, and mitigate the risks posed by cloud computing.
   2. The cloud risk management approach should be approved by the Board of the RE. The cloud risk management approach shall provide details regarding the various risks of cloud adoption such as technical, legal, business, regulatory 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.

3. As part of risk management process, a thorough risk assessment shall also be done keeping in mind that the RE cannot outsource the risks and decision making associated with deployment of cloud services, to the CSP. The risk assessment shall include (but not limited to) standards like identifying threat sources and events, identifying vulnerabilities and pre-disposing conditions, control analysis, magnitude of impact, etc.
4. A clearly identified and named resource (typically CISO) shall be appointed and shall be responsible for security of the deployments in cloud.

iii. **Compliance and Legal Aspects:** The RE shall have policies, processes, etc. in place to ensure compliance with the applicable legal and regulatory requirements (including but not limited to guidelines, circulars, advisories, etc.) for deployments in cloud, issued by SEBI/ Government of India/ respective state government.

iv. In order to ensure the smooth functioning and adherence with the GRC sub-framework, it is mandated to divide the roles and assign the responsibilities as given below:

1. *Role of the Board/Key Management Personnel (KMP)*- The Board/KMP shall be responsible for:
   a. Approval of cloud governance model and cloud risk management approach, and setting up processes 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 approach as per requirement of the RE. However, the review shall be mandatorily conducted at least once every year.
   c. Setting up the administrative responsibility of senior management.

2. *Role of Senior Management* - The senior management shall be responsible for:
   a. Preparation of and adherence with various policies related to cloud adoption.

b. Periodic assessment of cloud deployments and mitigation of risks arising out of the same.

c. Continually monitoring and responding to the risks and intimating 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 in order to assess its ability to continue to meet the various requirements such as legal, business, compliance, etc. and highlighting any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness to the 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 computing.

   ii. Capacity building within organization to build adequate skillsets to manage cloud deployments effectively.

3. *Role of IT team*- The IT team shall be responsible for managing day to day operations and assisting senior management in achieving the objectives of cloud deployments.

4. Additional roles/ responsibilities may be added (to the Board/KMP, Senior Management, etc.) as per requirements of the RE.

v. **Grievance Redressal Mechanism**: The 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'/ members' grievances related to cloud on boarded services shall rest with the RE. Adoption of cloud services shall not affect the rights of the investor/ member against the RE, including the ability of the investor/ member to obtain redressal of grievances 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) and service availability, adherence to SLA requirements, incident response mechanism, etc.
2. RE shall conduct regular audits/VAPT of its cloud deployments. The frequency and scope of such audits/VAPT shall be in line with SEBI cyber guidelines /circulars /framework issued from time to time.
3. Additionally, the RE shall also 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 having country of incorporation/registration outside of India, exposes the RE to country risk. To manage such risk, wherever applicable, 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. 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.

viii. **Contingency:** The RE shall have appropriate contingency and exit strategies. The RE shall ensure that availability of records to the RE and the supervising authority are not affected under any circumstances, even in case of liquidation of the CSP.

ix. **Miscellaneous**: Any other risk factors deemed relevant/ material by the RE.

Principle 2: Selection of Cloud Service Providers

2. Selection of CSPs:

The RE shall ensure that the following conditions are met while choosing any Cloud Service Provider (CSP):

i. 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 within the MeitY empaneled CSPs' data centers holding valid STQC (or any other equivalent agency appointed by Government of India) audit status.

ii. For selection of CSPs offering PaaS and SaaS services in India, the RE shall choose only those CSPs which:

1. Utilize the underlying infrastructure/ platform of only MeitY empaneled CSPs for providing services to RE.

2. Host the application/ platform/ services (DC, DR, near DR, etc.) provided to the RE as well as store/ process data of the RE, only within the data centers as empaneled by MeitY and holding a valid STQC (or any other equivalent agency appointed by Government of India) audit status.

3. Have a back-to-back, clear and enforceable agreement with their partners/ vendors/ sub-contractors (including those that provide the underlying infrastructure/ platform) for ensuring their compliance with respect to the requirements provided in this framework including those in Principles 6 (Security Controls), 7 (Contractual and Regulatory Obligations) and 8 (BCP, Disaster Recovery & Cyber resilience).

iii. Any other additional criteria that the RE considers appropriate/ as per RE's requirement.

iv. The RE shall ensure that storage/ processing/ transfer of its data should be done according to requirements provided in this framework as well as any other regulations/ circulars/ guidelines issued by SEBI and any other Government authorities.

Principle 3: Data Ownership and Data Localization

3. Data Ownership and Localization:

i. **Data Ownership:** The RE shall retain the complete ownership of all its data and logs, encryption keys, etc. residing in cloud. The CSP shall be working only in a fiduciary capacity. Therefore, the RE, SEBI and any other Government authority authorized under law, shall always have the right to access any or all of the data at any or all point of time.

ii. **Visibility**: Whenever required (by RE/ SEBI), the CSP shall provide visibility to RE as well as SEBI into CSP's infrastructure and processes, and its compliance to applicable policies and regulations issued by SEBI/ Government of India/ respective state government.

iii. **Data Localization**:
In order to ensure that RE and SEBI's right to access RE's data as well as SEBI's rights of search and seizure are not affected by adoption of cloud services, the storage/ processing of data (DC, DR, near DR etc.) including logs and any other data/ information pertaining to RE in any form in cloud shall be done as per the following conditions:

1. The data should reside/be processed within the legal boundaries of India.
2. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data/ transactions/ logs, available and easily accessible in legible and usable form, within the legal boundaries of India.

The RE shall ensure that the above-mentioned requirements are fulfilled at all times during adoption/ usage of cloud services.

iv. It is to be noted that the REs 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/ Government of India/ respective state government. Accordingly, RE shall put in place effective mechanism to continuously monitor the CSP and comply with various regulatory, legal and technical requirements notified by SEBI or any other Government authority from time to time.

Principle 4: Responsibility of the Regulated Entity

4. Responsibility of the RE (with respect to CSPs):

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 services adopted by it 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 applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ 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 "joint/ shared 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.

iii. In the event of a Managed Service Provider (MSP) or System Integrator (SI) being involved in procurement of cloud services, an explicit and unambiguous delineation/ demarcation of responsibilities shall also be done with respect to MSP/ SI, and the same shall be included in the agreement (in-line with the requirements given above).

iv. Similarly, there shall be an explicit and unambiguous delineation/ demarcation of responsibilities between the RE and CSP (and MSP/SI wherever applicable) for ensuring compliance with respect to applicable circulars (for example cybersecurity and cyber resilience circular, outsourcing circular, BCP-DR etc.) issued by SEBI from time to time. There shall be no "joint/ shared ownership"

for ensuring compliance with respect to any clause. If compliance for any clause has to be jointly ensured by RE and CSP (and MSP/SI wherever applicable), there should be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub-task/ line-item within the clause. This delineation shall also be added explicitly in the agreement (as an annexure) signed between the RE and the CSP (and MSP/SI wherever applicable).

v. In view of the fact that a CSP is not a RE, the RE shall continue to have ultimate responsibility and liability for any violation of the laws, rules, regulations, circulars, etc. issued by SEBI or any other authority under any law, regardless of any delineation/ demarcation of responsibilities envisaged in the aforesaid paragraphs.

Principle 5: Due Diligence by the Regulated Entity

5. Due Diligence by the RE (with respect to CSPs):

i. The REs should evaluate the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing. The RE shall also conduct its due diligence with respect to CSPs beforehand and on a periodic basis to ensure that legal, regulatory, business 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.

ii. A proper due diligence process should be established to assess the capabilities and suitability of a cloud service provider before the engagement.

iii. An analysis (including but not limited to comparative analysis, SWOT analysis, etc.) shall also be conducted on the type of cloud model to be adopted. The analysis should include relevant factors like (including but not limited to) the risks associated with various models, need, suitability, capability of the organization, etc. The above mentioned evaluations / analyses should be conducted keeping in mind that although the IT services/ functionality can be outsourced (to a CSP), REs are ultimately accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of RE's data and logs, and ensuring RE's compliance with respect to the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same.

iv. The criteria that an RE shall look out for are (including but not limited to):

1. Financial soundness of CSP and its ability to service commitments even under adverse conditions.

2. CSP's capability to identify and segregate RE's data, whenever required.

3. Security risk assessment of the CSP.

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

5. CSP's ability to effectively service all the RE's customers while maintaining confidentiality, especially where a CSP has exposure to multiple entities.

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

7. RE shall ensure that CSP performs proper screening and background checks of its personnel and vendors before onboarding, and provides adequate trainings and awareness programs to ensure that the customer (RE) services are not hampered due to misconfiguration/inadvertent actions/operational issues/etc.

8. Capability of the CSP to deal with RE's compliance needs, operational aspects, and ensure information security, data privacy, etc.

9. CSP's ability to ensure compliance with this framework as well as all applicable rules/ regulations/ circulars issued by SEBI from time to time.

10. Any other additional criteria that the RE considers appropriate/ as per RE's requirement.

Principle 6: Security Controls

6. Security Controls[4]:

The RE shall ensure its compliance with the applicable circulars (for example cybersecurity circular, systems audit circular, DR-BCP circular, etc.)/ guidelines/ advisories, etc. issued by SEBI. Further, in reference to the security controls for adoption of cloud computing[5], the following (including but not limited to) shall be implemented:

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 needs to check are given below:

i. *Vulnerability Management and Patch Management*:

1. 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 (i.e. managed by the CSP). The RE shall assess and ensure that the patch management of CSP adequately covers the components for which the CSP is responsible (i.e. components managed by the CSP). The patch management framework shall include the timely patching of all components coming under the purview of CSP.
2. The RE shall also ensure that CSP conducts Vulnerability Assessment and Penetration Testing (VAPT) for the components managed by the CSP and fixes the issues/ vulnerabilities within the prescribed timelines (as agreed upon by CSP and RE).
3. The RE shall also ensure that the vulnerability management, patch management and VAPT processes are conducted by CSP in-line with the requirements (for example scope, classification of vulnerabilities,

[4] For CSPs offering PaaS/ SaaS services, in the event any particular security control does not apply to their specific deployment model, such CSPs have to ensure that their vendor/ partner/ sub-contractor providing the underlying infrastructure/ platform fulfils the requirement of the security controls. The RE shall deploy the services of only those PaaS/ SaaS providers which have a back-to-back, clear and enforceable agreement with their vendor/ partner/ sub-contractor for the same.

[5] An indicative mind-map of security controls for cloud deployments is given in Appendix-B

duration for closure, etc.) provided in applicable circulars/ guidelines issued by SEBI.

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. The reporting should be done in-line with the guidelines/ regulations/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and RE.

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*[6]: Wherever the user management is done by CSP, the RE shall ensure that role based access and rule based access are strictly followed by CSP for its resources and it shall be based on the principle of least privilege. The following shall also be ensured:

[6] Any type of access/ user provided to SEBI/ any law enforcement agency of Government of India or state government shall be exempt from this clause

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. With respect to administrative privileges/ users, the following shall also be followed:
   a. 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.

   b. Access to systems or interfaces that could provide access to the RE's data is granted only if the RE has given explicit time-limited permission for that access.

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

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

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 use) 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 notified to the RE (as per the norms/ guidelines/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and 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. All conditions and obligations of the RE and CSP under this framework shall also be applicable in multi-tenancy structure.

vii. The RE shall ensure that the agreement with the CSP contains clause(s) for safe deletion/ erasure of RE's information. The clause should cover various scenarios like business requirement of RE, exit strategy, etc.

viii. For further assurance, the RE may assess the availability of global compliance standards like SOC-2[7] reporting for CSP.

ix. RE shall ensure that CSP has adequate controls (for example anti-virus, encryption of data, micro-segmentation, etc.) in place to safeguard cloud infrastructure as well as to 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.

[7] SOC-2 is a voluntary compliance standard for information security developed by American Institute of Certified Public Accountants (AICPA).

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 (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 components managed by RE shall be up to date in terms of patches/OS/version etc. The patch management policy shall also mandate timely patch application.

6.2.2. Vulnerability Assessment and Penetration Testing (VAPT):

The VAPT activity undertaken by RE should cover the infrastructure and applications/services hosted by the RE on cloud. 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. Additionally, the VAPT activity shall be conducted as per the requirements (including scope, classification, duration for closure of vulnerabilities, etc.) provided in applicable circulars/ regulations issued by SEBI.

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. SOC solution (in-house, third-party SOC or a managed SOC) of RE shall be integrated with the services/ application/ infrastructure deployed by RE in cloud. The continuous monitoring shall be done in an integrated manner and the services/ application/ infrastructure deployed in cloud should be treated as an extension of the RE's on premise network. 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. REs shall ensure that PII/sensitive data should not be shipped to the SOC.

6.2.4. Continuous Monitoring:

Continuous monitoring shall be done by the RE to review the technical, legal and regulatory compliance of CSP and take corrective measures/ ensure CSP takes 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 as well as by RE):

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 applicable 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 shall be adopted wherever feasible.

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

6.2.6. Security of Interfaces:

Controls related to 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)/ Multi Factor Authentication (MFA). For additional security, measures such as dedicated lease lines may be explored. The access logs and access list to the interface should be strictly monitored (by RE and CSP). 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 on the 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 shall also 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 shall be adopted, wherever necessary, to secure such interfaces.

6.2.7. Secure Software Development:

The RE shall undertake Secure Software Development practices for development of cloud-ready applications which shall include (but not limited to):

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

ii. A new approach for secure software development shall be implemented by RE for dealing with cloud native development concepts such as micro services, APIs, containers, server less architecture, etc. as the traditional security mechanisms 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 for development and usage of APIs. End to end security of the APIs shall also be taken care by the RE as per standard practices and guidelines.

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

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 clearly defined in the Agreement/Contract.

ii. As there are new risks introduced in engaging MSP/SI or both, the same shall be assessed, and mitigated 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 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 any sensitive data is in transit.

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

ii. To ensure RE's controls on encryption and Key management, the following shall be followed:

1. Wherever applicable:
   a. "Bring Your Own Key" (BYOK) 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.

   b. "Bring Your Own Encryption" (BYOE) approach shall be followed by the RE.

2. In case BYOK and BYOE approaches (as given above) are not implemented by RE, the RE shall conduct a detailed risk assessment and implement appropriate risk mitigation measures to achieve equivalent functionality/ security to BYOK and BYOE approaches.

3. Generating, storing and managing the keys in a Hardware Security Module (HSM) shall be implemented in a dedicated HSM to have complete control of Key management. 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 in the nature of anti-virus, Data Leak Prevention (DLP) solution etc. are installed and configured on the cloud deployments for effective data security. The RE shall also evaluate the baseline security controls provided by the CSP and may demand additional controls (from CSP) if required.

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 shall also consider the option of utilizing Cloud Access Security Broker (CASB)/ Secure Access Service Edge (SASE)/ similar frameworks or tools for effective monitoring of network, 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/UAT environment to ensure that the malware infection in such systems does not percolate to backup environment.
iii. Wherever CSP's backup services are utilized, adequate care should be taken with encryption solution and Key management.

6.2.13. Skillset:

RE shall equip staff overseeing cloud operations with the knowledge and skills required to securely use and manage the risks associated with cloud computing. The skills should also 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 will increase the reliability of services.

6.2.14. Breach Notification:

CSP shall notify the RE of any cybersecurity incident (for example data breach, ransomware, etc.) as mandated by the RE. The reporting shall be done as per the norms/ guidelines/ circulars issued by SEBI/ Government of India and (wherever applicable) as per the contractual agreement signed between the CSP and 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/ Government of India/ respective state government.

Principle 7: Contractual and Regulatory Obligations

7. Contractual and Regulatory Obligations[8]:

i. A clear and enforceable cloud service provider engagement agreement should be in place to protect RE's interests, risk management needs, and ability to comply with supervisory expectations.

ii. The contractual/agreement terms between RE and CSP shall include the provisions for audit, 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 its ability to manage risks, provide supervision and comply with regulatory requirements is not hampered by the contractual terms and agreement with CSP.

iii. 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. The agreement should also provide RE the right to intervene with appropriate measures to meet legal and regulatory obligations.

iv. SEBI/ CERT-In/ any other government agency shall at any time:
   1. Conduct direct audits and inspection of resources of CSP (and its sub-contractors/ vendors) pertaining to the RE or engage third party auditor to conduct the same and check the adherence with SEBI and government guidelines/ policies/ circulars and standard industry policies.
   2. Perform search and seizure of CSP's resources storing/ processing data and other relevant resources (including but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI authorized personnel/ agency 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.

[8] With respect to CSPs offering PaaS/SaaS services, REs shall deploy the services of only those CSPs which have a back-to-back, clear and enforceable agreement with their vendor/ partner/ sub-contractor providing their underlying infrastructure/ platform for fulfilling the requirements provided in this Principle.

3. Engage a forensic auditor to identify the root cause of any incident (cyber security or other incidents) related to RE.
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. Additionally, RE shall also include provisions (in the contract/ agreement with CSP) mandating that CSP extends full cooperation to SEBI while conducting the above-mentioned activities.

v. The RE shall also ensure that adequate provisions are included in the agreement/ contract for the following audit/ VAPT functions-
   1. CSP shall be responsible for conducting audit/ VAPT of the services/ components managed by the CSP.
   2. The RE shall be responsible for conducting audit/ VAPT of the services/ components managed by the RE. The audit/ VAPT shall be conducted as per the requirements (including scope, duration for closure of vulnerabilities, etc.) provided in various applicable circulars/ regulations issued by SEBI from time to time.
   3. Implementation and configuration audit of the resources to be deployed by the RE in cloud environment shall be conducted by the RE and the same shall be certified by the RE after closing all non-compliances/ observations before go-live.
   4. The RE may take into consideration the report/certificate of the audit of the CSP conducted by STQC. However, wherever required, CSP has to conduct additional audits (from CERT-In empaneled auditors) to fulfil all the requirements provided in various applicable circulars/ regulations issued by SEBI, and the same shall be ensured by the RE.
   5. The RE shall ensure that appropriate clauses/ terms (including SLA clauses) are added in the agreement (signed between RE and CSP) to enforce the above-mentioned audit/ VAPT requirements.

vi. Contract/Agreement should have adequate provisions regarding the termination of contract with CSP, and appropriate exit strategies to ensure

smooth exit without hindering any legal, regulatory or technical obligations of the RE.

vii. 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, CSP shall securely and permanently erase the RE's 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/ Government of India/ 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.

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

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

x. The agreement/contract made by RE shall also include (but not limited to) below mentioned terms/ provisions/ clauses:
    1. Definition of the IT activities and resources being on boarded on cloud, including appropriate service and performance standards including for the material 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 provisions, 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 (RE) data.
6. The deliverables, including SLAs, for formalizing the performance criteria to measure the quality and quantity of service levels.
7. Storage of data (as applicable to the RE) within the legal boundaries of India as per extant regulatory requirements.
8. Clauses requiring the CSP to provide details of data (captured, processed and stored) related to RE and RE's customers to SEBI/ any other government agency.
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, insolvency, etc. and indemnities, remedies, and recourse available to the respective parties.
12. Contingency plan(s) to ensure business continuity planning, RPO/RTO, and recovery requirements.
13. Provisions to fulfill the search and seizure requirements (as provided above in this principle) and audit/ VAPT requirements (as provided above in this principle).
14. Right to seek information (by RE/ SEBI) 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 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 cases involving the RE as and when required.
19. Clauses for performing risk assessment by CSP with respect to hiring of third party vendors, the checks/ process followed by CSP before onboarding personnel/ vendors, etc.
20. Any other provision(s) required to ensure compliance with respect to circulars/ guidelines/ regulations (including this cloud framework) issued by SEBI.

xi. 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 RE"* of the framework) for each task/ activity/ function. There shall be no "joint/ shared ownership" for any task/ activity/ function/ component.

xii. If any function/ task/ activity has to be performed jointly by the RE and CSP/MSP/SI, there shall be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) 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 (and MSP/SI wherever applicable). However, any such clause in the agreement shall not absolve the RE from having the ultimate responsibility and liability for any violation of the laws, rules, regulations, circulars, etc. issued by SEBI or any other authority under any law, regardless of any delineation/ demarcation of responsibilities.

xiii. Similarly, there shall be an explicit and unambiguous delineation/ demarcation of responsibilities between the RE and CSP (and MSP/SI wherever applicable) for ensuring compliance with respect to applicable circulars (for example

cybersecurity and cyber resilience circular, outsourcing circular, BCP-DR etc.) issued by SEBI from time to time. There shall be no "joint/ shared ownership" for ensuring compliance with respect to any clause. If compliance for any clause has to be jointly ensured by RE and CSP (and MSP/SI wherever applicable), there should be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub-task/ line-item within the clause. This delineation shall also be added explicitly in the agreement (as an annexure) signed between the RE and the CSP.

xiv. **Reporting Requirements**:

1. It is being reiterated that the RE is solely accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring RE's compliance with the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government.
2. The RE shall explicitly and unambiguously specify the party (RE or CSP/MSP/SI) which is responsible for ensuring compliance with each clause of the applicable SEBI circulars (for example cybersecurity circular, systems audit, etc.) in its audit reports. There shall be no "joint/ shared 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.
3. The RE shall ensure that the demarcation/ delineation of responsibilities is provided for each clause of the applicable SEBI circular(s).
4. In view of the above requirements, as well as to ensure effective monitoring of cloud deployments by REs, reporting of compliance (with this framework) shall be done by the REs in their systems audit, cybersecurity audit and VAPT reports, and it shall be done in the standardized format notified by SEBI from time to time.
5. **Reporting by Auditor**: As part of system audit of the RE, the auditor shall verify, and certify, whether there is a clear delineation/ demarcation of roles

and responsibilities between the RE and CSP/MSP/SI (in-line with the "*Principle 4: Responsibility of the RE*" of the framework):

a. For each task/ function/ activity/ component (including the tasks/ functions stated in clause (x) above, wherever applicable).
b. For each clause of applicable/ relevant SEBI circular/ guidelines/ regulations.

The auditor shall also verify, and certify, whether the above-mentioned demarcations of roles and responsibilities have been incorporated in the agreement/ contract signed between the RE and CSP (and MSP/SI wherever applicable).

xv. In the event of any CSP deployed by an RE losing its empanelment status with MeitY/ commits a passive breach of contract/ agreement in any way, the RE shall ensure that it becomes compliant with this framework within 6 (six) months of being notified of/ discovering the breach.

Principle 8: BCP, Disaster Recovery & Cyber Resilience

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

   i. The RE shall assess its BCP framework and ensure that it is in compliance with this cloud framework as well as other guidelines/ circulars issued by SEBI from time to time.

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

   iii. Additionally, RE shall develop a viable and effective contingency plan to cope with situations involving a disruption/ shutdown of cloud services.

Principle 9: Vendor Lock-In and Concentration Risk Management

9. Concentration Risk Management

i. RE shall assess its 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 also be assessed on a periodic basis.

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

iii. The RE shall also take measures to implement data portability and inter-operability as part of exit/ transfer strategy.

iv. In order to mitigate the risk arising due to failure/ shutdown of a particular CSP, and to limit the impact of any such failure/ shutdown on the securities market, SEBI may specify concentration limits on CSPs (thereby setting a limit on the number of REs that a CSP may provide its services to).

10. Recommendations:

i. RE may opt for any model of deployment on the basis of its business needs and technology risk assessment. However, compliance should be ensured with this cloud framework as well as other rules/ laws/ regulations/ circulars made by SEBI/ Government of India/ respective state government.

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

iii. While deploying cloud services, the REs shall adopt the nine (9) principles as provided in this framework:

1. Principle 1: Governance, Risk and Compliance Sub-Framework
2. Principle 2: Selection of Cloud Service Providers
3. Principle 3: Data Ownership and Data Localization
4. Principle 4: Responsibility of the Regulated Entity
5. Principle 5: Due Diligence by the Regulated Entity
6. Principle 6: Security Controls
7. Principle 7: Contractual and Regulatory Obligations
8. Principle 8: BCP, Disaster Recovery & Cyber Resilience
9. Principle 9: Vendor Lock-in and Concentration Risk Management

The REs shall ensure that their cloud deployments are compliant, in letter and spirit, with the above-mentioned principles.

iv. The cloud services shall 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. For selection of CSPs offering PaaS and SaaS services in India, RE shall choose only such CSPs which:

1. Utilize the underlying infrastructure/ platform of only MeitY empaneled CSPs for providing services to the RE.

2. Host the application/ platform/ services provided to RE, and store/ process data of the RE, only within the data centers as empaneled by MeitY and holding a valid STQC (or any other equivalent agency appointed by Government of India) audit status.
3. Have a back-to-back, clear and enforceable agreement with their partners/ vendors/ sub-contractors (including those that provide the underlying infrastructure/ platform) for ensuring their compliance with respect to the requirements provided in this framework including those in Principles 6 (Security Controls), 7 (Contractual and Regulatory Obligations) and 8 (BCP, Disaster Recovery & Cyber resilience).

v. There should be an explicit and unambiguous delineation/ demarcation of responsibilities for all activities (technical, managerial, governance related, etc.) of the cloud services between the RE and CSP (and MSP/SI wherever applicable). There shall be no "joint/ shared 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 (and MSP/SI wherever applicable) 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 (and MSP/SI wherever applicable).

vi. Similarly, there should be an explicit and unambiguous delineation/ demarcation of responsibilities between the RE and CSP (and MSP/SI wherever applicable) for ensuring compliance with respect to circulars (for example cybersecurity and cyber resilience circular, outsourcing circular, BCP-DR etc.) issued by SEBI from time to time. There shall be no “joint/ shared ownership” for ensuring compliance with respect to any clause. If compliance for any clause has to be jointly ensured by RE and CSP (and MSP/SI wherever applicable), there should be a clear delineation and fixing of responsibility between the RE and the CSP (and MSP/SI wherever applicable) for each sub-task/ line-item within the clause. This delineation shall also be added explicitly

in the agreement (as an annexure) signed between the RE and the CSP (and MSP/SI wherever applicable).

vii. As part of system audit of the RE, the auditor shall verify, and certify, whether there is a clear delineation/ demarcation of roles and responsibilities between the RE and CSP/MSP/SI (in-line with the "Principle 4: Responsibility of the RE" of the framework):

a. For each task/ function/ activity/ component.
b. For each clause of applicable/ relevant SEBI circular/ guidelines/ regulations

The auditor shall also verify, and certify, whether the above-mentioned demarcations of roles and responsibilities have been incorporated in the agreement/ contract signed between the RE and CSP (and MSP/SI wherever applicable.

viii. The contractual/agreement terms between RE and CSP shall include the provisions for audit, 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 its ability to manage risks, provide supervision and comply with regulatory requirements is not hampered by the contractual terms and agreement with CSP.

ix. SEBI/ CERT-In/ any other government agency shall at any time:

1. Conduct direct audits and inspection of resources of CSP (and its sub-contractors/ vendors) pertaining to the RE or engage third party auditor to conduct the same and check the adherence with SEBI and government guidelines/ policies/ circulars and standard industry policies.
2. Perform search and seizure of CSP's resources storing/ processing data and other relevant resources (including but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI authorized personnel/ agency 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) related to RE.
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. Additionally, RE shall also include provisions (in the contract/ agreement with CSP) mandating that CSP extends full cooperation to SEBI while conducting the above-mentioned activities.

x. The cloud framework should be read along with the circulars (including circulars on outsourcing, cybersecurity, BCP-DR, etc.), directions, advisories, etc. issued by SEBI from time to time.

xi. Transition Period:

1. For the REs which are not utilizing any cloud services currently, the framework shall be applicable/ come into force from the date of issuance.
2. For the REs which are currently utilizing cloud services, upto 12 months shall be given to ensure their compliance with the framework. Additionally, such REs shall provide regular milestone-based updates as follows:

SN.	Timeline	Milestone
1	Within one (1) month of issuance of framework	REs shall provide details of the cloud services, if any, currently deployed by them.
2	Within three (3) months of issuance of framework	The REs shall submit a roadmap (including details of major activities, timelines, etc.) for the implementation of the framework
3	From three (3) to twelve (12) months of issuance of framework	Quarterly progress report as per the roadmap submitted by the RE.

4	After twelve (12) months of issuance of framework	Compliance with respect to the framework to be reported regularly

3. The above-mentioned reporting shall be done to the authority as per the existing mechanism of reporting for systems audit/ cybersecurity audit.

xii. The compliance with respect to the framework shall be submitted by the REs as part of their systems audit, cybersecurity audit, and VAPT reports, and no separate reporting is envisaged. The reporting shall be done as per the standardized format notified by SEBI from time to time. All other conditions for reporting (for example reporting authority, duration of reporting, etc.) shall be as per the existing mechanism of reporting for systems audit/ cybersecurity audit/VAPT.

Appendix-A

Format for Submission of Details of Cloud Deployments

The REs shall provide details of their cloud deployment in the following format-

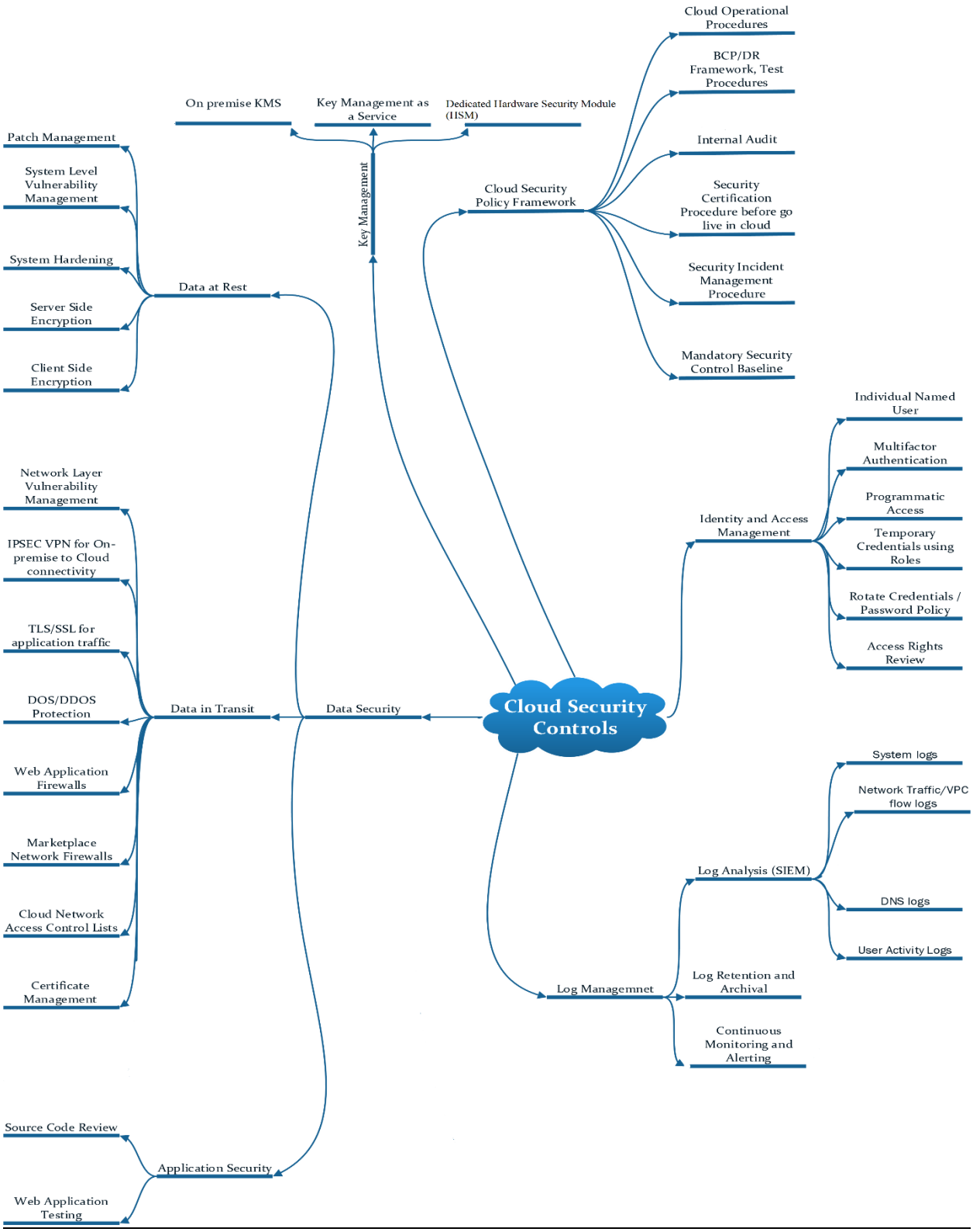
A. Entity Name:

B. Entity Type: (For example stock exchange, depository, mutual fund, etc.)

C. Whether Utilizing Cloud Services? Yes/ No

For Each Cloud application/ service/ system, please provide a response to the following:

SN	Details Required	***Entity Response***
1	Name of the Application/ Service/ System	
2	The type of deployment model utilized (public cloud, community cloud, etc.)	
3	The type of service model utilized (For example IaaS, PaaS, etc.)	
4	Name of the Cloud Service Provider (CSP)	
5	Country of incorporation/ registration of CSP	
	Name of the Managed Service Provider (MSP) / System Integrator (SI) [wherever applicable]	
6	Country of incorporation/ registration of MSP/ SI	
7	Whether the application/ service/ system is a critical or core application/ service/ system?	
8	Details of Data hosted/ stored in cloud	
9	Whether data is stored within the legal boundaries of India?	

Appendix-B

Indicative Mindmap for Cloud Security