14 November 2022

To:
Securities and Exchange Board of India
Ms. Shweta Banerjee (DGM-ITD)
Submitted via email to: cloud_framework@sebi.gov.in

RE: ASIFMA response SEBI Consultation Paper on Cloud Framework

Dear Sir/Madam,

ASIFMA[1] is grateful for the opportunity to respond to the Securities and Exchange Board of India ("SEBI") Consultation Paper on Cloud Framework ("Consultation Paper")[2].

Our members[3] are global firms with many of them rolling out global cloud migration projects. As India is a key market for many of our members, we are keen to work with you to ensure that global financial institutions ("FIs") can implement their global cloud strategies in the India to enable them and the Indian markets to benefit from all the advantages cloud can bring.

In what follows, we provide some overarching suggestions, followed by more detailed feedback on some of the articles in the Consultation Paper.

Application to public cloud (IaaS and PaaS) only

We note that SEBI had articulated the various cloud deployment models within this Consultation Paper (page 8). For the purposes of this cloud framework, industry would like to confirm that this cloud framework applies to public cloud deployment only, namely the IaaS (where the RE has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) and PaaS models (where the RE has control over the deployed applications and possibly configuration settings for the application-hosting environment). We understand that this draft framework will not apply to a SaaS model since the RE only manages limited user-specific application configuration settings. This is aligned with the definitions provided in page 8 of the Consultation Paper.

---

[1] *ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.*

[2] SEBI, 2022: https://www.sebi.gov.in/reports-and-statistics/reports/nov-2022/consultation-paper-on-cloud-framework_64661.html

[3] *https://www.asifma.org/membership/members/*

If SEBI intends to implement this framework across all types of public cloud deployments, we recommend that SEBI allow firms to take a risk-based approach and calibrate the controls based on the risks presented by the cloud deployment.

Internal cloud

We submit that the draft framework should only be applicable to public cloud, and not internal/private cloud. It is common for FIs to adopt internal cloud, i.e., one shared "utility" affiliate entity centrally providing internal cloud to service affiliated banks, securities, asset management entities and other affiliated FIs across multiple jurisdictions in the same group. The use of internal cloud is simply an internal automation and streamlining of how an FI manages its own hardware and data centers, in order to increase flexibility and resilience, and, as such, it does not involve third-party infrastructure, nor does it increase cyber risk. This is aligned with the definitions (cloud model descriptions, including private cloud) provided on page 8 of the Consultation Paper.

Legal application

We appreciate that SEBI noted on page 4 that the nine principles are "suggested high-level principles" and we interpret it as a set of guidelines that REs may refer to when adopting public cloud solution on a risk-based approach and are not mandatory requirements for REs to adopt. If there are controls which are mandatory as indicated in page 4, we recommend that SEBI denote which are mandatory provisions.

Principles and risk-based approach

Technology and public cloud adoption are fast evolving and adopting the Cloud Framework on a principles and risk-based basis, would allow FIs flexibility to adopt evolving control measures that best fit their risk profile and benefit from future developments and innovation. Listing examples or prescribing specific tools within the Cloud Framework could make the document outdated when new tools emerge. Across the provisions within this framework, we seek that SEBI allows firms to take a risk-based approach and implement the controls proportionate to the risks presented and the criticality of the application and services provided.

We seek that SEBI does not require the granular controls stipulated within this draft framework to be mandatory so that firms can evolve their controls and adapt to changing technology.

Taking a principle and risk-based approach would be in line with the HKMA Cloud Guidance[4] and Monetary of Authority Singapore's 2021 Advisory[4] that addresses the technology and cyber security risks associated with public cloud adoption. The advisory outlines non-mandatory risk management principles and best practice standards to guide FIs in Singapore in managing the risks of public cloud adoption.

Risk assessment

For the list of security controls under principle 6, we are confirming that firms can adopt a risk-based approach and REs could leverage CSPs' third-party audit reports and certifications. We welcome SEBI explicitly allows firms to use SOC2 reports for assessment and would like to confirm that firms are not required to validate controls already tested in SOC2 reports or any other third-party audit report and certifications which are conducted to provide to CSP clients an independent assessment of CSPs control environment relevant to system security, availability and confidentiality and more. We recommend that

[4] HKMA, 2022: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220831e1.pdf

SEBI make it clear that REs are able to reference any and all of CSP's audit reports and certifications (as noted for SOC2 in Principle 6 VIII) as evidence and not require REs to perform additional audit against a CSP for the same requirements. If CSPs are subject to multiple audit requests from multiple REs throughout the year for the same things. This is an inefficiency and does not reduce risk. Furthermore, some of these operational controls are not open for public testing due to sensitive nature of the environment and that it's a shared tenancy type responsibility. Overall, the requirements under principle 6 are also prescriptive and move away from a principles and risk-based approach.

Recognition of global firms' global cloud arrangement

We respectfully request SEBI not to impose local data storage and processing requirement for reasons outlined below.

Global firms are rolling out global cloud migration projects. As India is a key market, it is of utmost importance that global FIs can implement their global cloud strategies in India in a way that is consistent and limits frictions. Free movement of data across border is key to roll out global cloud migration projects. Global FIs typically consolidate their systems in a single global hub, which offers services to the rest of the firm. In contrast, local data storage/processing require discrete technological builds, further segregating local systems from global hubs. This exposes FIs to greater cybersecurity risks by creating a more decentralised environment that needs to be safeguarded, which further inhibits central oversight and information sharing across borders. In addition, local processing will negatively impact FIs' global operation, their ability to undertake activities at a global level and cross-border service offering.

The financial sector is committed to providing SEBI with timely access to data needed to fulfill SEBI's regulatory and supervisory mandate no matter where the data is stored, this is also a principle widely adopted in international trade agreements[5] and financial regulatory community[6]. As an example, Monetary Authority of Singapore signed Data Connectivity initiatives with the US Treasury, the Bangko Sentral ng Pilipinas (BSP) and the Swiss State Secretariat for International Finance (SIF)[7]. Those Data Connectivity initiatives recognize the importance of cross border data connectivity in financial services in economic growth and the development of innovative financial services, risk management and compliance programs. Conversely, data localisation requirements may increase cybersecurity risks and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to data. The Data Connectivity Initiatives enable data flows (including personal information) within financial groups or with business partners, across borders by electronic means provided this activity is for the conduct of the business within the scope of their license, authorisation, or registration; and supports the free choice of location for the storage and processing of data as long as financial regulators or supervisors have appropriate access to data necessary to fulfill their regulatory or

[5] Example, Article 17.18 in the United States-Mexico-Canada Agreement.

[6] Example, United States-Singapore Joint Statement on Financial Services Data Connectivity.

[7] MAS-UST Joint Statement on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity
MAS-BSP Joint Statement on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas
MAS-SIF Joint Statement of Intent on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2022/joint-statement-of-intent-between-the-monetary-authority-of-singapore-and-the-swiss-state-secretariat-for-international-finance-to-promote-data-connectivity-for-financial-services

supervisory mandate[8]".Therefore, we respectfully request SEBI not to impose local data storage and processing requirement global firms.

Recognize global firm's firmwide cloud governance approach

Several areas within this paper such as audits, cloud governance framework, and cloud strategy must take into account the operating model of foreign global firms in India. Given that this framework is implemented on REs in India, we are confirming that for global firms that rely on firmwide cloud arrangements, they may rely on firmwide cloud audit results to fulfil the audit requirements, as well as their global technology risk management and technology and cybersecurity frameworks and strategy.

Shared responsibility

We welcome SEBI's use of the term "shared responsibility" in this paper. SEBI's position on clearly delineating responsibilities between CSPs and REs is aligned with industry practice. But we note that the interpretation of shared responsibility within this paper differs from the definition described in financial regulators' guidelines and the industry's understanding. We encourage SEBI to align the definition of shared responsibility in this paper with the widely used definition.

In the 'shared responsibility model', both the FI and the CSP take responsibility for activities, such as security and compliance, that are required for running a public cloud service. The CSP manages elements such as the provision of servers, networking, and data centre facilities, whilst the FI is responsible for aspects such as customer data, security, application management and user access. This model can also extend to sharing responsibilities for IT controls and risk management requirements (for example, both parties owning and managing access controls for areas which they are responsible for). Nevertheless, this shared responsibility model does not mean that FIs discharge their ultimate accountability on CSPs, as the ultimate liability for any FI activity will always be held by the FI.

The MAS Cloud Advisory provides a clear segregation of the Shared Cybersecurity Responsibilities between FIs and CSPs. In general, CSPs are responsible for "Security-of-the-Cloud", FIs would be responsible for "Security-in-the-Cloud". In the advisory, MAS articulates:

a. *"Security-of-the-Cloud" refers to the security of the public cloud services under the CSPs' responsibility. In an IaaS or PaaS arrangement, these would typically include the security of the underlying hardware, system software and the hypervisor. For SaaS, this would also include the underlying security of the application software.*
b. *"Security-in-the-Cloud" refers to the security of the cloud workloads under the FIs' responsibility. In an IaaS or PaaS arrangement, these should typically include securing IT systems components such as applications, operating system and orchestration tools. In a SaaS arrangement, it would generally include managing user account privileges and data access rights."'*

The Shared Cybersecurity Responsibility approach is a principles-based approach that varies in implementation depending on the service model, for example, the delineation of responsibilities would differ for IaaS, PaaS, or IaaS.

[8] https://www.mas.gov.sg/news/media-releases/2022/joint-statement-of-intent-between-the-monetary-authority-of-singapore-and-the-swiss-state-secretariat-for-international-finance-to-promote-data-connectivity-for-financial-services

Useful resources on Shared Responsibility:

1. CSA's Cloud Control Matrix (CCM) - The CSA CCM is a cybersecurity control framework for cloud computing (https://cloudsecurityalliance.org/research/cloud-controls-matrix/)
    a. It is composed of 197 control objectives structured in 17 domains covering all key aspects of cloud technology.
    b. It is a tool for the systematic assessment of cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain.
    c. The controls framework is aligned to the CSA Security Guidance for Cloud Computing, and is considered a de-facto standard for cloud security assurance and compliance
2. The financial sector developed the FSP Cloud Extension[9] that provides guidance to FIs and CSPs on commonly understood responsibilities related to cloud deployment across SaaS, PaaS, and IaaS delivery models. It helps clarify where a firm's responsibilities end and a CSPs responsibilities begin.

Cloud Risk

Risks that come from the use of cloud should not be treated any differently from other third-party risks because this approach could create fragmented third-party risk management practices and increase operational burden. We recommend that SEBI enable FIs to leverage existing operational risk management, outsourcing, resilience and cybersecurity framework, instead of developing a new cloud-specific framework. If gaps are identified, the existing operational risk management frameworks can be adapted to include new risks posed or existing risk associated with cloud adoption.
The current Draft Framework seems to assume that cloud services present different risks than data centre outsourcing, which may not be the case.

Please find below further detailed feedback and suggestions on some of the provisions in the draft Cloud Framework. We hope that you find our feedback useful and that it will be positively considered and reflected in the final Framework.

We would very much welcome further engagement with SEBI on the draft Framework over a virtual meeting or in-person meeting when the ASIFMA team will be in Mumbai on 21-24 November.

Best regards,

Laurence Van der Loo
Executive Director, Technology & Operations
Asia Securities and Financial Markets Association

[9] Cyber Risk Institute: https://cyberriskinstitute.org/the-profile/ (first document)

Text	Issues	Proposals/ Suggestions/ Changes	Rationale/ Context/ Remarks
Executive Summary 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.	We agree with SEBI that the RE should be ultimately accountable for the use of cloud applications (and this is in line with the views of other global regulators such as the UK PRA). We are however concerned about the level of access from CSPs that is expected as many stipulations in the draft Framework require a level of control and ownership and also access into CSPs that Res do not necessarily have and/or that are very difficult to achieve as part of contractual discussions with the CSPs and which go far beyond current practice for public cloud. REs are responsible for the availability of its applications in the cloud, confidentiality, integrity and security of its data and logs pertaining to its own application and infrastructure. CSPs are responsible for its own infrastructure. A clear delineation of responsibility is useful here. : e.g. "not limited to availability of cloud applications, confidentiality,	We strongly suggest SEBI to remove such prescriptive requirements and allow FIs to adopt a risk-based approach, and allow FIs to rely on third party audits and external certifications for the CSPs.	Ensure practicality and implementability of the Cloud Framework.

	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". This level of access to the CSP particularly as principles 6 and 9 seem to exclude the ability for REs to use existing certifications. (states "For further assurance, the RE may assess the availability of SOC-2 reporting of CSP").		
Executive Summary 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.	The types of encryption methods implemented by REs depends on the types of data, its level of sensitivity, and the type of usage. Prescribing encryption across the lifecycle is not practical for REs. For example, data needs to be in decrypted form when it is processed or used. Moreover, as technology evolve quickly, these types of prescriptive requirements may soon be outdated.	We strongly suggest SEBI to remove such prescriptive requirements and allow FIs to adopt a risk-based approach	Ensure an implementable cloud framework.

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.	NA	NA	NA
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.	NA	NA	NA
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.	This current draft contains new requirements, that if are mandatory, will require reconfiguring REs' existing cloud deployment models.	We recommend a longer lead time for REs to comply with requirements in this framework, with a minimum of 18 months.	To determine feasibility.
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.	NA	NA	NA

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.	Items under E are not due diligence process.	We propose changing the title to "Considerations before the adoption of cloud based services"	For clarification.
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	We are concerned that despite being high level principles, the requirements of the security controls is prescriptive and not principles and risk-based.	As mentioned in the body of our letter, we are confirming that this framework is a high-level guideline and SEBI will indicate parts of the provisions which are mandatory, calibrated against the different types of public cloud models.	Technology evolves fast and controls may become outdated. REs should be given the flexibility to adapt the controls they take based on evolving technology.
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.	While item (1) is about cloud strategy, item (2) and (4) refers to third party governance. The Board also does not work in isolation on a framework, it should recognize the role of senior management too.	We would like to clarify what is meant by cloud governance model, whether it refers to a cloud strategy or a third-party governance framework for cloud , and recognize the role of senior management in forming any governance frameworks	For clarification
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.	The controls that are used to address risks in the use of cloud is the same as other types of third-party risks. Hence, it is redundant to have a separate cloud risk management sub-framework as it is managed by the tech and cyber, and third party risk frameworks used by firms. On the appointment of a CISO, many global financial firms leverage global or regional teams and we note that the appointed CISO may be based outside of India.	Risks that come from the use of cloud should be treated as third-party risks. We are confirming that REs can leverage its existing tech, cyber and third-party risk management framework.	The treatment of the risks that come with the use of cloud like other third-party risks is in line with the US Office of the Controller of the Currency's position, that is, that public cloud is a third-party relationship and third-party risk management for cloud computing is fundamentally the same as for other third-party relationships. The same position is adopted by the Financial Stability Board in its 2019 "Third-party dependencies in cloud services" report. The MAS also relies on its Outsourcing Supervisory Policy Manual for various types of third-party outsourcing, including cloud.
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	NA	NA	NA

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.	Global firms leverage their existing cyber and tech risk management framework, as well as their third-party risk management framework. And we are confirming that global firms can leverage this approach for the cloud governance and cloud risk management framework, and they can determine the frequency of approval and reviews based on a risk-based approach.	We are confirming SEBI's recognition of firmwide methodology adopted by global firms and that local RE's board can endorse the frameworks that are put together by the global headquarters. On item (a) we are confirming that the approval and review process can be determined by the REs through a risk-based approach and based on the criticality of the workload.	For clarification.
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.	Firms take a risk-based approach to determine the periodic assessment, based on criticality of the workload.	We are confirming that REs can take a risk-based approach and determine the frequency of assessment for items b and d for the types of public cloud deployment based on criticality.	For clarification.

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.	NA	NA	NA
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.	NA	NA	NA
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.	We suggest that the existing SCORES[10] platform should be sufficient and should be leveraged to comply with this requirements.	We suggest that SEBI clarifies that SCORES platform is sufficient.	Avoid unnecessary duplicated requirements.
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.	Global firms have firmwide arrangements when it comes to audits of cloud deployments.	We are confirming that for global firms that rely on firmwide cloud arrangement, the Indian REs may rely on firmwide cloud audit results to fulfil the audit requirements.	For clarification
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.	NA	NA	NA
Principle 2: Data Residency and Sovereignty			

[10] https://scores.gov.in/scores/Welcome.html

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.	Free movement of data across borders is key to rolling out global cloud migration projects. Global FIs typically consolidate their systems in a single global hub, which offers services to the rest of the firm. In contrast, data localisation policies require discrete technological builds in specific jurisdictions, further segregate local systems from global hubs. This exposes FIs to greater cybersecurity risks by creating a more decentralised environment that needs to be safeguarded, which further inhibits central oversight and information sharing across borders. In addition, local processing will negatively impact FIs' global operation, their ability to undertake activities at a global level and cross-border service offering. Principle 2 as currently drafted seems to indicate that global FIs would have to move workloads from global services into India if they want to use CSP services. This would significantly reduce the incentive to use	We recommend the removal of localization requirements to enable FIs to undertake activities at a global level and cross-border service offering. Before prescribing such requirements, we seek that SEBI shares its concerns with industry so that we can come to an alternative solution such as focusing on data access instead of data localisation. Whilst being a suboptimal outcome, if removal of data localisation requirements is not possible, the type of data which should reside in India should be specifically confirmed to make the draft Framework implementable. Additionally, processing should be allowed outside India. Additionally, for RE's that may currently be utilising non-MeitY empaneled CSPs, we would request SEBI to offer a grace period of implementation to allow REs to serve the remaining period of their contracts prior to migrating to a MeitY empaneled CSP. Such grace period should be determined based on the	The financial sector is committed to providing SEBI with timely access to data needed to fulfill SEBI's regulatory and supervisory mandate no matter where the data is stored, this is also a principle widely adopted in international trade agreements and financial regulatory community. Therefore, we respectfully request SEBI not to impose local data storage and processing requirement global firms. The need to focus on access versus localization (specifically in the context of cloud) was also recognized the Hong Kong SFC in their FAQs pertaining to their Circular on the Use of External Data Storage, and following extensive industry engagement.

	a CSP and as such negatively impact innovation in India's capital markets. Also, Standardisation Testing and Quality Certification (STQC) is not a global standard and existing application vendors are already facing challenges in getting STQC for their applications, which are used by the Regulated Entities of SEBI. Prescribing such requirements would further hinder FIs from benefitting from cloud solutions	respective RE's contractual agreement to avoid any breach of commercial agreement and to ensure that proper migration planning is put in place to avoid any unwanted operational challenges and risks.	
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.	Data ownership: "RE shall retain complete ownership of its data and associated data, encryption keys, logs etc. residing in cloud." This combined with principle 6.2.9 that states that REs would need BYOK , BYOE (bring your own encryption) with HSMs on prem to support the encryption, is problematic, especially when REs wish to utilize PaaS/SaaS type services of the CSP that do not support such approach regarding the logs and encryption keys, thereby limiting REs to	We suggest to remove the requirements to maintain compete ownership of keys and logs for PaaS services. As mentioned in the intro remarks on page 1 above, we assume that SaaS services are out of scope for this Framework.	Ensure a well-calibrated and implementable cloud framework and allow REs to use PaaS and SaaS services.

	mainly to fundamental IaaS services.		
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.	Allowing to check the integrity of the cloud computing services and compliance is a level of access CSPs have rarely if ever given to any client.	SEBI to clarify that this obligation does not fall under RE.	Ensure an implementable cloud framework
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.	*" RE shall put in place effective mechanism to continuously monitor the CSP/MSP/SI and comply with various regulatory, legal and technical requirements."* If interpreted strictly, this would require the REs to deploy controls to monitor the infrastructure of the CSP. To our knowledge this has never happened on a public CSP.	Suggest to remove this requirement.	Ensure an implementable cloud framework
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.	NA	NA	NA
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/	NA	NA	NA

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.	Industry's implementation of the shared responsibility model is aligned with SEBI's expectation of clearly delineating responsibilities between CSPs and REs.	We propose removing the line 'There shall be no "shared responsibility" or "joint ownership" for any function/ task/ activity between the RE and CSP.' since industry's definition of shared responsibility may differ. Moreover, even without this statement, it is quite clear that SEBI expects clear segregation of responsibilities between CSPs and REs.	For clarification.
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	NA	NA	NA

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:	NA	NA	NA
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:	NA	NA	NA
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,	NA	NA	NA

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.	NA	NA	NA
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.	This requirement seems to conflict with 6.2.9 (ii) and (iii).	We suggest to remove 6.1 (iv).	Remove conflicting requirements.
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.	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. 4. The necessary auditing and monitoring of the same shall be done by CSP and any anomalies shall be reported to the RE." This is not applicable in case of IaaS, where the PIDs are managed by the Regulated Entities.	Calibrate the requirement for IaaS	Ensure and implementable cloud framework.

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.	The immediate notification requirement may be difficult to put in practice. When an incident occurs, it takes time for service providers to understand the impact and whether it reaches a materiality threshold for incident reporting.	We recommend the use of the term "without undue delay of any incident having a substantial impact on the provision of a service" instead of "immediately". In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account: (a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities.	For feasibility.

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, backup cartridges and any other permanent memory devices etc.) the CSP should destruct/erase data permanently before leaving the premises of CSP.	NA	NA	NA
viii. For further assurance, the RE may assess the availability of SOC-2 reporting of CSP.	NA	NA	NA
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.	NA	NA	NA
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:	NA	NA	NA
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.	NA	NA	NA
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.	We would like to clarify that the responsibility to conduct VAPT on applications and services fall on REs, and the responsibility to conduct VAPT on the CSP's infrastructure fall on the CSPs as they own the infrastructure. A clear delineation of responsibility is useful here.	Clarify that REs are responsible for VAPT of its own applications, and CSPs are responsible for VAPT of its infrastructure. A clear delineation of responsibility is useful here.	For clarification so that the framework is developed based on what is feasible.

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.	" SOAR" should not be used as it relates to a product or class of products whilst other products may be able to achieve the same objective and it should be left for the FIs to decide.	Replace with term "automated actions"	Technology-neutral, risk-based approach.
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.	NA	NA	NA
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.	NA	NA	NA
6.2.6. Security of Interfaces: Typical interfaces in a cloud deployment are given below:	NA	NA	NA
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.	NA	NA	NA

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.	"*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*" – all of those are names of products, not of capabilities. Regulation should avoid the use (even in examples) of terms which represent products and instead list the requirements that those products should achieve.	Language to be revised accordingly, as there are different ways to achieve the desired security.	We seek that SEBI allows firms to take a risk-based approach and implement the controls based on the risks present. We seek that SEBI does not require the granular controls stipulated within this draft framework to be mandatory so that firms can evolve their controls and adapt to changing technology
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.	"*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*" – all of those are names of products not of capabilities. Regulation should avoid the use (even in examples) of terms which represent products and instead list the requirements that those products should achieve.	Language to be revised accordingly, as there are different ways to achieve the desired security.	We seek that SEBI allows firms to take a risk-based approach and implement the controls based on the risks present. We seek that SEBI does not require the granular controls stipulated within this draft framework to be mandatory so that firms can evolve their controls and adapt to changing technology

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.	We seek that SEBI allows firms to take a risk-based approach and implement the controls based on the risks present. We seek that SEBI does not require the granular controls stipulated within this draft framework to be mandatory so that firms can evolve their controls and adapt to changing technology.	We are confirming that the best practices in item iii are examples and are not mandatory for REs to implement.	For clarification.
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.	NA	NA	NA
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.	Hardware Security Module (HSM) that are cloud-based or those that are stored on-prem have similar specifications. Moreover, the storage of HSM is dependent on the cloud deployment model. Data-in-use i.e. wherever data that is being used or processed in the public cloud, confidential computing solutions shall be implemented.”, this would require applications redesign, most CSPs have	We recommend that SEBI allows REs to take a risk-based approach in determining where to use cloud-based or on-prem HSM and when to use confidential computing. We also seek elaboration on what is meant by “confidential computing solution”.	Provide REs with flexibility given advancement in technology has resulted in little difference in cloud-based or on-prem HSM.

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.	limited CCs servers and there are performance issues with enclave technology. "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." While the keys can be generated at the RE's premises, they need to be imported into the HSM provided by CSP to use in the Cloud. Hence, the guideline should be updated accordingly.		
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.	This would represent a significant cost for DLP for servers and DLP and endpoint security such as EDR would prevent using PaaS services such as container platforms.	Calibrate the requirements.	Ensure a cost-effective, implementable cloud framework.
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.	Cloud Access Security Boker (CASB) and Secure Access Service Edge (SASE) are commercial products.	Delete (ii)	Referring to specific (commercial) technologies is not aligned with a risk-based and technology-neutral approach. Such prescriptive references are also not calibrated to the actual requirements and take from the FIs the ability

			to decide on other tools that may be a better fit and future technologies that may be able to fulfil the underlying requirements better.
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.	NA	NA	NA
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.	NA	NA	NA
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.	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 – this does not place any requirements on the CSP to deliver the information without undue delay, but the REs are required to report "immediately". We recommend a calibration of timelines to match.	CSP notification obligations to match those of RE, to ensure smooth info timelines.	To ensure smooth timelines.

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.	NA	NA	NA
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.	NA	NA	NA
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.	We would like to clarify under which circumstances the government agencies will perform search and seizure.	We encourage SEBI to clearly articulate the circumstances and the reference law and regulation. We hold the view that normal data requests relating to REs' data should come through the RE and not by SEBI or other government agencies going directly to the CSPs.	For clarification.
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.	NA	NA	NA
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	NA	NA	NA

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.	NA	NA	NA
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.	NA	NA	NA
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.	NA	NA	NA

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.	NA	NA	NA
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.	Industry's implementation of the shared responsibility model is aligned with SEBI's expectation of clearly delineating responsibilities between CSPs and REs.	We propose removing the last line. Moreover, even without this statement, it is quite clear that SEBI expects clear segregation of responsibilities between CSPs and REs.	For clarification.
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.	NA	NA	NA
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.	NA	NA	NA

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.	NA	NA	NA
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.	Industry's implementation of the shared responsibility model is aligned with SEBI's expectation of clearly delineating responsibilities between CSPs and REs.	We propose removing the terms "shared responsibility" or "joint ownership". Moreover, even without this statement, it is quite clear that SEBI expects clear segregation of responsibilities between CSPs and REs.	For clarification.
4. The RE shall ensure that the demarcation/ delineation of responsibilities is provided for each clause of the circular(s).	NA	NA	NA
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.	NA	NA	NA
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.	NA	NA	NA
Principle 9: Vendor Lock-In and Concentration Risk Management			
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-	Multi-cloud strategies and hybrid cloud strategies, while used for contingency and resilience, are primarily adopted for accessing unique services across CSPs.	We propose that item iii be tweaked to "The RE should also monitor for concentration risk arising from internal dependencies."	Sector wide concentration cannot be done by REs since they do not have visibility over what services are used by other REs. Sector wide

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.	While multi-cloud can reduce concentration risk to some extent, the technical, process and resource complexity needed to support multiple CSPs can lead to decreased resilience overall. It is important to differentiate between sector-wide concentration risk and internal dependency. We believe that assessment of concentration risk in the sector should be done by authorities in close partnership with the financial services industry. For risks of this nature, authorities (e.g., supervisory bodies) are well positioned to have oversight at an industry level	We propose the removal of "such as implementing a **multi-cloud ready** solutions". Migration from CSP to CSP currently takes significant time and effort – this is an industry wide issue. We would recommend that the regulator promotes and support the building and adoption of common architecture/baseline/protocol to ease migration.	concentration risk should be managed by the regulator. In seeking to mitigate systemic risk, it is important that authorities avoid placing additional complexity or restrictions on an FI's ability to make commercial decisions and adapt to emerging business models and technologies, as some solutions to address industry-wide concentration risk currently proposed by authorities may limit the FI's ability to make commercial decisions and adapt to emerging business models and technologies. As a useful reference, we would like to refer to the 2021 paper of our European sister association AFME, called "Building resilience in the cloud".[11]

[11] AFME, 2021: https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_CloudComputing2021_06-2.pdf