



Department: Technology

Segment: All Segments

Circular No: MSE/IT/16795/2025

Date: February 21, 2025

Subject: Advisory for Financial Sector Organizations Software as a Service(SaaS) based solutions(Half yearly from October 2024 to March 2025)

To All Members,

This is with reference to the SEBI Circular No. SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 dated November 03, 2020 “Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions”.

A copy of the report format is enclosed as **Annexure – I** for the period from October 2024 to March 2025 (Half Yearly).

Members are requested to take note of the same and arrange for compliance with the requirements specified in the said Circular and submit the report by April 30, 2025. The SEBI circular regarding Software as a Service (SaaS) based solutions is attached below as **Annexure-II**).

**For and on behalf of
Metropolitan Stock Exchange of India Limited**

**Laxmi Narayan Sahu
Chief Information Security Officer**

Annexure I

<<Member Name>>
<<Address>>
<<Email Address>>
<<Information Security Contact Person>>

“Compliance of the SEBI circular for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions”

Under guidance received from SEBI as per circular – SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 & subsequent Amber advisory from CERT-In – 201155100308.

<<Member Name>> would like to confirm that specified confidential data and data types (as specified in the CERT-In advisory) are **hosted / not hosted** on with SaaS provider / <<Member Name>> use or does not use any SaaS based GRC solutions. **Half-yearly report** for the period **October 2024 to March 2025**.

If Yes, kindly provide your responses in the below format.

CSP Name	Nature of service consumed	Environment usage (Including nature of data exchanged)	Geo-Location for hosting	Gaps against Circular	Deadline to close the Gaps

*CSP – Cloud Service Providers

Annexure II



CIRCULAR

SEBI/HO/MIRSD2/DOR/CIR/P/2020/221

November 03, 2020

To

**All Stock Brokers through exchanges
All Depository Participants through Depositories
All Merchant Bankers
All Registrar to an Issue and Share Transfer Agent
All Debenture Trustee
All Credit Rating Agencies
All Bankers to an issue
All STP Service Providers
All Approved Intermediaries**

Dear Sir/Madam,

Subject – Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions

1. Ministry of Electronics & Information Technology, Govt. of India (MoE&IT), has informed SEBI that the financial sector institutions are availing or thinking of availing Software as a Service (SaaS) based solution for managing their Governance, Risk & Compliance (GRC) functions so as to improve their cyber Security Posture. As observed by MoE&IT, though SaaS may provide ease of doing business and quick turnaround, but it may bring significant risk to health of financial sector as many a time risk and compliance data of the institution moves beyond the legal and jurisdictional boundary of India due to nature of shared cloud SaaS, thereby posing risk to the data safety and security.
2. In this regard, Indian Computer Emergency Response Team (CERT-in) has issued an advisory for Financial Sector organizations. The advisory has been forwarded to SEBI for bringing the same to the notice of financial sector organization. The advisory is enclosed at **Annexure A** of this circular.
3. It is advised to ensure complete protection and seamless control over the critical systems at your organizations by continuous monitoring through direct control and supervision protocol mechanisms while keeping the critical data within the legal boundary of India.

4. The compliance of the advisory shall be reported in the half yearly report by stock brokers and DP to stock exchanges and depositories respectively and by direct intermediaries to SEBI with an undertaking, "Compliance of the SEBI circular for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made."
5. The advisory annexed with this circular shall be effective with immediate effect.
6. 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.

Yours faithfully,

Anupma Chadha
Dy. General Manager
Phone:022-26449319
Email: anupmac@sebi.gov.in

Annexure A

TLP: AMBER

CERT-Fin Advisory- 201155100308

Advisory for Financial Sector Organisations – RBI and SEBI

Overview

It has been learnt that some of the financial sector institutions are availing or thinking of availing Software as a Service (SaaS) based solution for managing their Governance, Risk & Compliance (GRC) functions so as to improve their cyber security posture. Many a time the risk & compliance data of the institution moves cross border beyond the legal and jurisdictional boundary of India due to the nature of shared cloud SaaS. While SaaS may provide ease of doing business and quick turnaround, it also brings significant risk to the overall health of India's financial sector with respect to data safety and security.

Description

If the following data sets fall in the hands of an adversary/cyber attacker, it may lead to unprecedented increase in the attack surface area and weakening of Indian financial sector infrastructure's overall resilience.

- Credit Risk Data
- Liquidity Risk Data
- Market Risk Data
- System & Sub-System Information
- Internal & Partner IP Schema
- Network Topography & Design
- Audit/Internal Audit Data
- System Configuration Data
- System Vulnerability Information
- Risk Exception Information
- Supplier Information & it's dependencies related Data

Solution

The Financial Sector organisations may be advised to protect such critical data using layered defence approach and seamless protection against external or insider threat. The organisations may also be advised to ensure complete protection & seamless control over their critical system by continuous monitoring through direct control and supervision protocol mechanisms while keeping such critical data within the legal boundary of India.

The organisations may also be requested to report back to their respective regulatory authority regarding compliance to this advisory.

It is requested that you may kindly keep CERT-In informed of the actions taken and periodically provide the updated compliance to this advisory.

(It may be noted that TLP Amber means: Limited disclosure, restricted to participants' organizations.

When should it be used: Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

How may it be shared: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.)