National Stock Exchange of India Limited
Circular

DEPARTMENT: INSPECTION	
Download Ref No: NSE/INSP/74021	**Date: April 30, 2026**
Circular Ref. No: 22/2026	

To All ASPs,

Sub: Periodic submission of System, Cyber, and VAPT Audit by Application Service Provider (ASP)

Empaneled ASPs of the Exchange are required to conduct periodic system audit of the (Non-NEAT Frontend) NNF facility and security controls built in their ASP platform.

In order to strengthen the cybersecurity measures in securities market and to ensure adequate cyber resilience against cybersecurity incidents/attacks, empaneled ASP vendors are also required to conduct periodic Cyber Security Audit & VAPT assessment audit on yearly basis for cyber security related controls built in their ASP platform.

The timelines for the submission of preliminary audit report and action taken report for system, cyber and VAPT audit are given below:

Sr. No.	Report Type	Audit Period	Timelines for submission- Preliminary Audit Report	Action Taken Report (If Applicable)
1	System Audit Report	01st April to 31st March	On or before 30th June	On or before 30th September
2	Cyber Audit Report	01st April to 31st March	On or before 30th June	On or before 30th September
3	VAPT Report	01st April to 31st March	On or before 30th June	On or before 30th September

In view of the above ASP vendors are advised to take note of following guidelines for the conduct of System Audit, Cyber Audit and VAPT assessment.

- The guideline for selecting Auditors of ASP vendors in adherence to the prescribed Auditor Selection Norms for System Audit, Cyber Audit & VAPT assessment are enclosed as Annexure - A.
- Further, the format for System Audit & Cyber Audit Preliminary report & ATR for ASP vendor is enclosed as Annexure - B & Annexure – C respectively.
- The formats of Declaration from Auditor, Assessment Details(scope), VAPT Audit report/Summary, in accordance with SEBI CSCRF has been enclosed as Annexure - D & Annexure - E
- For System audit, Terms of Reference (TOR) of system audit is enclosed in Annexure - F
- For conduct of Cyber audit, Terms of Reference (TOR) of cyber audit is enclosed in Annexure - G.

Additionally, ASP Vendors are required to submit the System audit, Cyber audit & VAPT audit report after approval by Managing Director/Director/CTO or CISO.

In case of any query or support for the submission of the System audit, Cyber audit & VAPT audit report, please reach out us on email address: DL-SYSCYB@nse.co.in.

For and on behalf of
National Stock Exchange of India Limited

Prashant Aier
Chief Manager – Inspection

Enclosure:

Annexure A – Auditor selection Norms
Annexure B – System audit report format
Annexure C – Cyber audit report format
Annexure D – Auditor's declaration – VAPT Scope
Annexure E – Format for VAPT Summary report
Annexure F – Terms of Reference (TOR) applicable for System Audit
Annexure G – Terms of Reference (TOR) applicable for Cyber Audit

In case of any clarifications, Application Service Provider may contact our below offices:

Regional Office	E MAIL ID	CONTACT NO.
Ahmedabad (ARO)	inspectionahm@nse.co.in	079- 49008632
Chennai (CRO)	inspection_cro@nse.co.in	044- 66309915 / 17
Delhi (DRO)	delhi_inspection@nse.co.in	011- 23459127 / 38 / 46
Kolkata (KRO)	inspection_kolkata@nse.co.in	033-4040 0455/59
Mumbai (WRO)	compliance_wro@nse.co.in	022-26598200 / 022-61928200
Central Help Desk	compliance_assistance@nse.co.in	

Annexure-A

A. Auditor Selection Norms for System Audit

1. The Audit firm/LLP/Company having 3 years or more experience, can take assignment of conducting system audit of Trading Member/ASP Vendor. In addition, the Audit Firm/LLP/Company which undertakes the System Audit of shall have always at least three Partners/Directors having a valid CISA(ISACA)/ DISA(ICAI)/ CISM(ISACA) /CISSP(ISC2) Certification, of which at least two Partners/Directors should be full-time Partners/ Whole Time Directors. The partner of firm/ LLP/ director of company signing the audit report shall have 3 years or more experience in conducting system audit of Trading Member/ ASP vendors and shall have valid CISA(ISACA)/ DISA(ICAI)/ CISM(ISACA)/ CISSP(ISC2) Certification.
2. System Auditors meeting the above-mentioned criteria and empaneled with Exchange can be selected/appointed for conducting system audit. The list of System Auditor empaneled with NSE is available on the website at the following link.
   https://inspection.nseindia.com/empanelment_auditor/auditor/viewEmpanelledAuditors/
3. The Audit firm/LLP/Company can perform a maximum of 3 consecutive years audits of the ASP Vendor. However, such Audit firm/LLP /Company shall be eligible for reappointment after a cooling-off period of two years.
4. The ASP Vendor & Auditing Organization/Entity must not have any conflict of interest in conducting fair, objective and independent audit. It shall not have been engaged over the last two years in any consulting engagement with any departments/ units of the ASP vendor being audited.
5. The Action Taken Report, if applicable, shall be validated by the same auditor who conducted the system audit.
6. ASP Vendors are required to maintain comprehensive records of the audit team members who visit their premises for a minimum period of three years.
7. System Auditors shall preserve working papers, logs, screenshots, records of visits to the premises of the entity, POC and other evidence in support of the audit for a period not less than three years.

B. Auditor Selection Norms of Cyber Audit

1. Auditing Organization/Entity must mandatorily be CERT-In empaneled.
2. Auditor of Auditing Organization/Entity must preferably have a minimum of 3 years of experience in IT audit of Banking and Financial services, preferably in the Securities Market. E.g. Stock exchanges, clearing houses, depositories, stockbrokers, depository participants, mutual funds, etc. The audit experience should have covered all the major areas mentioned under various cybersecurity frameworks and guidelines issued by SEBI from time to time. Auditing experience of the Cybersecurity Framework under ISO 27001 for an organization will be an added advantage.
3. The Auditor of Auditing Organization/Entity must have experience in/ direct access to experienced resources in the areas covered under CSCRF. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security professional) from International Information systems Security Certification Consortium, commonly known as (ISC)2.
4. The Auditor of Auditing Organization/Entity shall have ISMS/ IT audit/ governance frameworks and processes conforming to leading industry practices.
5. The CERT-In empanelled Auditing Organization/Entity can perform a maximum 3 consecutive years audits of the ASP Vendor. However, such CERT-In empanelled Auditing Organization/Entity shall be eligible for reappointment after a cooling-off period of Two year.
6. The Auditor & Auditing Organization/Entity must not have any conflict of interest in conducting fair, objective and independent audit of the ASP. It shall not have been engaged over the last two years in any consulting engagement with any departments/ units of the ASP being audited.
7. The Auditor & Auditing Organization/Entity may not have any cases pending against its previous auditees, which fall under SEBI's Jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.
8. The Auditing Organization/Entity must compulsorily enter into a Non-disclosure Agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report subsequently should leave the jurisdiction of India.

C. Auditor Selection Norms for VAPT

1. Auditing Organization/Entity must mandatorily be CERT-In empanelled'.
2. The auditor of Auditing Organization/Entity must have experience of performing VAPT.
3. Auditor of Auditing Organization/Entity must preferably have a minimum 3 years of experience in IT audit of Banking and Financial services preferably in the Securities Market. E.g. Stock exchanges, clearing houses, depositories, stockbrokers, depository participants, mutual funds, etc. The audit experience should have covered all the major areas mentioned under various cybersecurity frameworks and guidelines issued by SEBI from time to time. Auditing experience of the Cybersecurity Framework under ISO 27001 for an organization will be an added advantage.
4. The Auditor of Auditing Organization/Entity must have experience in/ direct access to experienced resources in the areas covered under SEBI-CSCRF.
5. The Auditor of Auditing Organization/Entity shall have ISMS/ IT audit/ governance frameworks and processes conforming to leading industry practices.
6. The CERT-In empanelled Auditing Organization/Entity can perform a maximum of 3 consecutive audit years of the ASP Vendor. However, such CERT-In empanelled Auditing Organization/Entity shall be eligible for reappointment after a cooling-off period of Two year.
7. The Auditor & Auditing Organization/Entity must not have any conflict of interest in conducting fair, objective and independent audit of ASP Vendor. It shall not have been engaged over the last two years in any consulting engagement with any departments/ units of the ASP Vendor being audited.
8. The Auditor & Auditing Organization/Entity may not have any cases pending against its previous auditees, which fall under SEBI's Jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.
9. The auditor of Auditing Organization/Entity must compulsorily use only licensed tools.
10. The Auditing Organization/Entity must compulsorily enter into a Non-disclosure Agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report subsequently should leave the jurisdiction of India.

Annexure – B

System Audit Report Format

i. System Audit Preliminary Report

Sr. No.	TOR Clause	TOR Description	Description of finding/observation*	Status of Finding	Risk Rating	Impact Analysis	Deadline for corrective Action	ATR To Be Submitted (yes/no)	Management response in case of acceptance of associate risk/ASP Vendor Comments
1	**1**	**System Control and Capabilities**							
	1(a)	Order Tracking – The system auditor should verify system process and controls at API based terminals (CTCL/SOR/ IBT / STWT / DMA etc.) with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.							
		...							
N	23 (d)	...							

* **Note** – For TOR clause marked as 'Not Applicable', System Auditor provide a clarification/remark for non-applicability of said TOR.

Status of Finding – Compliant/Non-Compliant/Not-Applicable
Risk Rating – High/Medium/Low

ii. System Audit Action Taken Report (ATR)

Sr. No.	TOR Clause	TOR Description	Description of finding/observation	Initial Status of Finding	Status of finding as per the ATR	Risk Rating	ASP Vendor's Comment	Auditor's Comment
1	**1**	**System Control and Capabilities**						
	1(a)	Order Tracking – The system auditor should verify system process and controls at API based terminals (CTCL/SOR/ IBT / STWT / DMA etc.) with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.						
	...	...						
N	23(d)	...						

Status of Finding – Compliant/Non-Compliant/Not-Applicable
Risk Rating – High/Medium/Low

Annexure-C

Cyber Audit Report Format

i. Cyber Audit Preliminary Report

Sr. No.	TOR Clause	TOR Description	Description of finding/observation*	Status of Finding	Risk Rating	Impact Analysis	Deadline for corrective Action	ATR To Be Submitted (yes/no)	Management response in case of acceptance of associate risk/ASP Vendor Comments
1		**Governance**							
	1(a)	Has the ASP Vendor designated a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/Partners/Proprietor of the ASP Vendor? Is the reporting of the CISO directly to the MD & CEO of their organization? ... Is the level, grade, and standing of the CISO at least equivalent to CTO/CIO?							
		...							
n	23(A)(i)	...							

* Note- For TOR clause marked as 'Not Applicable', Cyber Auditor provide a clarification/remark for non-applicability of said TOR.

Status of Finding – Compliant/Non-Compliant/Not-Applicable
Risk Rating – Critical/High/Medium/Low

ii. Cyber Audit Action Taken Report (ATR)

Sr. No.	TOR Clause	TOR Description	Description of finding/observation*	Initial Status of Finding	Status of finding as per the ATR	Risk Rating	ASP Vendor's Comment	Auditor's Comment
1		**Governance**						
	1 (a)	Has the ASP Vendor designated a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/Partners/Proprietor of the ASP Vendor? Is the reporting of the CISO directly to the MD & CEO of their organization? Does the CISO possess sufficient qualification and capabilities to carry out his/her responsibilities? Has the ASP Vendor established a reporting procedure to facilitate communication of cybersecurity incidents/unusual						

Sr. No.	TOR Clause	TOR Description	Description of finding/observation*	Initial Status of Finding	Status of finding as per the ATR	Risk Rating	ASP Vendor's Comment	Auditor's Comment
		activities to the CISO or to the senior management in a time-bound manner as defined by guidelines/policies/laws/circulars/regulations, etc.? Is the level, grade, and standing of the CISO at least equivalent to CTO/CIO?						
		....						
n	23(A)(i)	..						

Status of Finding – Compliant/Non-Compliant/Not-Applicable
Risk Rating –Critical/High /Medium/Low

Annexure-D

Auditor's Declaration- VAPT Scope (required on auditor's letter head)

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Partner/Director/Proprietor of firm/Company <Name of the Auditing Organization> with CERT-In empanelment from <Date> to <Date>. I have conducted VAPT for <Name of the ASP> period <....> as per the requirements of SEBI/ Exchanges.The following scope of VAPT covered as per circulars/guidelines/ advisories issued by SEBI/Exchanges:

Scope VAPT:

S. No.	Assessment Area	Details (assets, applications, etc.) of the Audit area	Is the Entity Compliant? (Yes/ No)	Auditor's comments
1	VA of Infrastructure (Server, Storage, Network, etc) -Internal & External			
2	VA of Applications-Internal & External			
3	External Penetration Testing			
4	Wi-Fi Testing			
5	API Security Testing			
6	VA and PT of mobile applications			
7	Network segmentation testing			
8	OS and DB Assessment			
9	VAPT of cloud implementation			
10	Configuration audit of infrastructure (like i.e. operating systems, databases & middleware, network devices, security devices, cloud and firewall rule review etc.)			

*Note: Kindly provide the auditor's justification in "Auditor's comments" column for the VAPT scope marked as not applicable.

I confirm that the VAPT has been conducted as per guidelines/norms prescribed in the Circular. I also confirm that I have no conflict of interest in undertaking the above-mentioned VAPT activity.

For and on behalf of
Name:
Contact no.:

Place: Date:

Annexure - E

Format for VAPT Summary Report

VAPT Report Summary				
Name of ASP Vendor				
Contact person Details (Name, Mobile number & Email ID) of ASP Vendor (Preferably CISO's)				
VAPT Completion Date "(DD-MM-YYYY)"				
Date of approval of VAPT report by or MD/CISO/CTO/Director of ASP Vendor "(DD-MM-YYYY)"				
Name of the Auditor				
Name of the Audit Firm				
Audit Firm Landline No.				
Auditor Mobile No.				
Auditor / Audit Firm Email ID				
CERT-In empanelment validity expiry Date "(DD-MM- YYYY)"				
Risk	**Critical**	**High**	**Medium**	**Low**
(A) No of closed vulnerabilities				
(B) No of open vulnerabilities as on Report Date				
Reason for non-closure: Mention for Critical, High, Medium, and Low separately				
Vulnerabilities planned to be closed by "(DD/MM/YYYY)" *				
Remarks				
*Note - Any gaps/vulnerabilities detected shall be remedied in a risk-based approach. Further, ATR/compliance report of closure of findings identified during VAPT shall be submitted within 3 months post submission of VAPT report. The planned target date should be mentioned accordingly. The VAPT summary needs to be digitally signed by ASP Vendor and the auditor.				

ASP Vendor Name:	
ASP Vendor's Authorised Signatory:	
Auditor Name/Firm Name:	
Auditor/Firm Sign:	

Annexure – F

Terms of Reference (TOR) applicable for System Audit

Audit TOR Clause	TOR Details
1	**System Control and Capabilities**
1(a)	Order Tracking – The system auditor should verify system process and controls at API based terminals (CTCL/SOR/ IBT / STWT / DMA etc.) with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.
1(b)	Order Status/ Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.
1(c)	Rejection of orders – Whether system has capability to reject orders which do not go through order level validation at the end of the ASP Vendor (CTCL/SOR/ IBT / STWT / DMA etc.) and at the servers of Exchange.
1(d)	Communication of Trade Confirmation / Order Status – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log for IBT / STWT / DMA.
1(e)	Client ID Verification – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.
1(f)	Order type distinguishing capability –Whether system has capability to distinguish the orders originating from CTCL / IBT / STWT / DMA/etc.. . Whether CTCL / IBT / STWT / DMA / etc. orders are having unique flag/ tag as specified by the Exchange and systems identify the orders emanating from CTCL / IBT / STWT/ DMA/etc. by populating the 15-digit CTCL field in the order structure for every order. Whether Broker/ASP is using similar logic/ priorities as used by Exchange to treat CTCL / IBT / STWT /DMA /etc. client orders
1(g)	The installed system parameters are as per Exchange norms: • Approved CTCL / IBT / STWT / DMA / etc. Software Name and Version No (as applicable) and • Strategy Name & Version No. • Software developed by • Order Gateway Version • Risk Administration / Manager Version • Front End / Order Placement Version

Audit TOR Clause	TOR Details
	Provide address of the CTCL / IBT / DMA / STWT server location (as applicable).
1(h)	The installed system (viz. CTCL/ IBT / STWT / DMA/) features are as prescribed by the Exchange. Main Features Price Broadcast The system has a feature for receipt of price broadcast data Order Processing : The system has a feature : • Which allows order entry and confirmation of orders • which allows for modification or cancellation of orders placed • Trade Confirmation • The system has a feature which enables confirmation of trades The system has a feature which provides history of trades for the day to the user
1(i)	Execution of Orders / Order Logic Execution of Orders / Order Logic The installed system provides a system based control facility over the order input process Order Entry The system has order placement controls that allow only orders matching the system parameters to be placed. Order Modification The system allows for modification of orders placed. Order Cancellation The system allows for cancellation of orders placed. Order Outstanding Check The system has a feature for checking the outstanding orders i.e. the orders that have not yet traded or partially traded.
1(j)	The installed system (viz. CTCL/ IBT / DMA / STWT system) parameters are as per Exchange norms Gateway Parameters • • Trader ID • Market Segment - CM • • CTCL ID • • IP Address • • Exchange Network • Leased Line ID • Market Segment – F&O • • CTCL ID • • IP Address

Audit TOR Clause	TOR Details
	• • Exchange Network • • Leased Line ID • Market Segment – CDS • • CTCL ID • • IP Address • • Exchange Network • Leased Line ID • Market Segment – CO • • CTCL ID • • IP Address • • Exchange Network • Leased Line ID
1(k)	Trades Information The installed CTCL system provides a system based control facility over the trade confirmation process the Trade Confirmation and Reporting Feature : • Should allow confirmation and reporting of the orders that have resulted in trade • The system has a feature which provides history of trades for the day to the user
1(l)	System Auditor to check whether DMA facility has been offered to only those categories of investors which have been permitted by the Stock Exchange. System Auditor to Refer Clause 2.2.3.1. Chapter 2 of SEBI master circular SEBI/HO/MRD2/PoD-2/CIR/P/2023/171 dated October 16, 2023 and Section 6.2.2.of NSE consolidated circular NSE/MSD/61825 dated April 30, 2024
1(m)	System Auditor to check whether ASP vendor has system / policy in place to ensure that only clients who fulfill the eligibility criteria are permitted to use the DMA facility. System Auditor to Refer Clause 2.2.6.1. Chapter 2 of SEBI master circular SEBI/HO/MRD2/PoD-2/CIR/P/2023/171 dated October 16, 2023.
1(n)	System Auditor to check whether ASP vendor has complied with the testing guidelines as mentioned in Exchange Cir No- NSE Circular NSE/MSD/61081 dated March 12, 2024, on review of usage of Non-Neat Frontend (NNF) products
2	**Software Change Management - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**
2(a)	Processing / approval methodology of new feature request, change or patches
2(b)	Change Management Process, related approvals, Version Control- History, etc. For change requests, whether the changes are tested before being approved for deployment into production. Whether the categorization of the change is done properly?
2(c)	Fault reporting / tracking mechanism and process for resolution

Audit TOR Clause	TOR Details
2(d)	Testing of new releases / patches / modified software / bug fixes Does demonstratable segregation exists between Development / Test / Production environment
2(e)	The System Auditor to check whether adequate mechanism to restore their trading systems to 'production state' at the end of testing session so as to ensure integrity of trading system.
2(f)	New release in production – promotion, release note approvals
2(g)	Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.
2(h)	User Awareness
2(i)	The system auditor should check whether critical changes made to the CTCL / IBT / STWT / ALGO / DMA /etc.. are well documented and communicated to the Stock Exchange.
2(j)	Change Management To ensure system integrity and stability all changes to the installed system are planned, evaluated for risk, tested, approved and documented. Has the organisation implemented a change management process to avoid risk due to unplanned and unauthorised changes for all the information security assets (Hardware, software, network, application)? Does the process at the minimum include the following? Planned Changes Are changes to the installed system made in a planned manner? a) Are they made by duly authorized personnel? b) Risk Evaluation Process c) Is the risk involved in the implementation of the changes duly factored in? Change Approval Is the implemented change duly approved and process documented? Pre-implementation process Is the change request process documented? Change implementation process Is the change implementation process supervised to ensure system integrity and continuity Post implementation process Is user acceptance of the change documented?

Audit TOR Clause	TOR Details
	Emergency Changes In case of emergency changes, are the same duly authorized and the manner of change documented later? Are Records of all change requests maintained? Are periodic reviews conducted for all the changes which were implemented?
2(k)	Patch Management Does the organization have a documented process/procedure for timely deployment of patches for mitigating identified vulnerabilities? Does the organisation maintain a tracker for the deployed, failed or missing patches along with the dates of the patch being applied? Whether version and patch management controls are in place? Does the organization periodically update all assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS Desktops etc. with latest applicable versions and patches? Ensure that the critical system (servers, network devices, Endpoints) are replaced before they reach End-of-Life or End-of-Support and no EOL/EOS systems are present in the ASP's environment.
2(l)	SDLC - Application Development & Maintenance In case of ASPs self-developed system SDLC documentation and procedures if the installed system is developed in-house
2(m)	SDLC - Application Development & Maintenance Does the organization has any in house developed applications? If Yes, then Does the organization have a documented process/framework to include processes for incorporating, testing and providing sign-off for information risk requirements at various stages of Software Development Life Cycle (SDLC)? Does the SDLC framework incorporate standards, guidelines and procedures for secure coding? Are roles and responsibilities clearly defined for various stakeholders in the SDLC framework? Are Application development, Testing (QA and UAT) and Production environments segregated?
2(n)	Changes undertaken pursuant to a change to the stock Exchanges trading system.
2(o)	The auditor should check that ASP Vendors are not using software without requisite registration of stock Exchange and there has not been any unauthorized change to the registered software.
3	**Risk Management System (RMS)**
3(a)	Online risk management capability – The system auditor should check whether the system of online risk management (including upfront real-time risk management) is

Audit TOR Clause	TOR Details
	in place for all orders placed through CTCL terminals (CTCL / IBT/STWT /DMA etc.). The System auditor shall further check whether all orders emanated through CTCL terminals (CTCL / IBT/STWT /DMA etc.) subjected to the prescribed risk management system prior to execution and no order bypasses the risk management system. (Number of orders generated should be equal to orders routed through the Risk Management System of the ASP.)
3(b)	Trading Limits –Whether a system of pre-defined limits / checks such as Single Order Quantity and Single Order Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order value Limit, Order Price limit, Spread order quantity and value limit, Cumulative open order value check (unexecuted orders) are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.
3(c)	Order Alerts and Reports –Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to Margin Requirements, payments and delivery obligations.
3(d)	Order Review –Whether the system has capability to facilitate review of such orders that were not validated by the system (CTCL / IBT/ STWT/ DMA/ SOR).
3(e)	Back testing for effectiveness of RMS – Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.
3(f)	Log Management – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.
3(g)	Order Reconfirmation Facility The installed CTCL system/ Non-Neat Frontend (NNF) system provides for reconfirmation of orders which are larger than that as specified by the member/ASP risk management system. The system has a manual override facility for allowing orders that do not fit the system based risk control parameters
3(h)	Settlement of Trades The installed CTCL system/ Non Neat Frontend (NNF) system provides a system based reports on contracts, margin requirements, payment and delivery obligations Margin Reports feature

Audit TOR Clause	TOR Details
	Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations.
3(i)	Information Risk Management Has the organization implemented a comprehensive integrated risk assessment, governance and management framework? Has the organization developed detailed risk management program that incorporates standards, guidelines, templates, processes, risk catalogues, checklist, measurement metrics and calendar to support and evidence risk management activities? If yes, is the risk management program calendar reviewed periodically? Are the risk identification and assessment processes repeated periodically to review existing risks and identify new risks Are risks reported to the Senior Management through reports and dashboards on a periodic basis? Are evidences available to demonstrate risk decisions such as Risk Mitigation, Risk Acceptance, Risk Transfer, Risk Avoidance by senior management. Is there a dedicated Risk Management Team for managing Risk and Compliance activities? Is the Risk Management Framework automated? Are SLA's defined for all risk management activities? Has the organization defined procedure/process for Risk Acceptance? Are reports and real time dashboards published in order to report/track Risks?
3(j)	Has the organization deployed alert mechanism for detecting malfunctioning of device, software and backup system?
3(k)	All ASP should have system in place to calculate all obligations of client such as margin obligation/ client position etc. during the day on the basis of various files (trade files, margin parameters file and settlement price file) being provided by Clearing Corporation/Exchange.
4	**Password Security**
4(a)	Organization Access Policy – Whether the organization has a well-documented policy that provides for a password policy as well as access control policy for the CTCL/ Non-Neat Frontend (NNF) systems.
4(b)	Authentication Capability – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.

Audit TOR Clause	TOR Details
4(c)	Password Best Practices – Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.
4(d)	The installed CTCL/Non Neat Frontend (NNF) Facility system Authentication mechanism is as per the guidelines of the Exchange The installed CTCL/Non Neat Frontend (NNF)/IBT/STWT system used password for authentication. The password policy/standard is documented. The installed systems password features includes: a) The installed system uses passwords for authentication. b) The system requests for identification and new password before login into the system. c) The Password is masked at the time of entry. System authenticates user with a User Name and password as first level of security. System mandates changing of password when the user logs in for the first time? Automatic disablement of the user on entering erroneous password on five consecutive occasions. The system provides for automatic expiry of passwords at the end of a reasonable duration (maximum 90 Days) and re-initialisation of access on entering fresh passwords. Prior intimation is given to the user before such expiry? System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical. System controls to ensure that the changed password cannot be the same as of the last 6 passwords. System controls to ensure that the Login id of the user and password should not be the same. System controls to ensure that the password should be of minimum six characters. User/Client is deactivated if the same is not used for a continuous period of 24 (Twenty four) months from date of last use of the account as per the Exchange circular no. NSE/INSP/64718. System allows user to change their passwords at their discretion and frequency. System controls to ensure that the password is encrypted at ASP's end so that employees of the ASP cannot view the same at any point of time.
5	**Session Management (Mobile Application / Applicability Client Server Application / Web Application)**

Audit TOR Clause	TOR Details
5(a)	Session Authentication – Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.
5(b)	Session Security – Whether there is availability of an end-to-end encryption for all data exchanged between client and ASP vendor systems. or other means of ensuring session security Whether session login details are stored on the devices used for IBT, STWT and DMA only.
5(c)	Inactive Session – Whether the system allows for automatic trading session logout after a system defined period of inactivity.
5(d)	Log Management – Whether the system generates and maintains logs of Number of users, activity logs, system logs, Number of active clients.
5(e)	The installed system has provision for security, reliability and confidentiality of data through use of encryption technology. a) The system uses SSL/TLS or similar session confidentiality protection mechanisms b) The system uses a secure storage mechanism for storing of usernames and passwords c) The system adequately protects the confidentiality of the user's trade data.
5(f)	Cryptographic Controls : Does the organization have a documented process/framework for implementing cryptographic controls in order to protect confidentiality and integrity of sensitive information during transmission and while at rest, using suitable encryption technology? Is the encryption methodology of information involved in business transactions based on Regulation/Law/Standards compliance requirements? Does the organization ensure Session Encryption for internet-based applications including the following? Does the organization ensure that the data transferred through internet is protected with suitable encryption technologies? Are transactions on the website suitably encrypted?
5(g)	Cryptographic Controls Is secret and confidential information sent through e-mails encrypted before sending? Is secret and confidential data in an encrypted format?
5(h)	Does the organisation have a data leakage prevention (DLP) solution/ process? Is the DLP configured/ deployed across all the endpoints (end users), email and network? Are relevant policies/ rules configured on the DLP to prevent exfiltration of PII data, sensitive and confidential data from within the organisation and organisational assets? Does the DLP solution / process support alerting / blocking of movement of data from within the organisation to an unauthorised external domain?

Audit TOR Clause	TOR Details
6	**Database Security**
6(a)	Access – Whether the system allows CTCL/Non-Neat Frontend (NNF) - database access only to authorized users / applications.
6(b)	Controls – Whether the CTCL/Non-Neat Frontend (NNF) database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.
6(c)	Data at rest is encrypted
7	**Network Integrity**
7(a)	Seamless connectivity – Whether ASP vendor ASP Vendor has ensured that a backup network link is available in case of primary link failure with the exchange.
7(b)	Network Architecture – The ASP should have detailed network architecture diagram delineating exchange connectivity along with the backup links to showcase failover, clear portrayal of internet service providers, segregation of different zones (Production, UAT, DMZ, etc.). The network diagram should also depict the internal and external flow of network traffic. The version control should be maintained for the Network Diagram. The Network Architecture diagram should be periodically reviewed or in case of any changes to the infrastructure. The Network Architecture diagram should also be approved by the Technology Committee.
7(c)	Firewall Configuration – Whether appropriate firewall is present between ASP vendor trading setup and various communication links to the exchange. Whether the firewall default configuration settings are changed and is appropriately configured to ensure maximum security
7(d)	Network Security Are networks segmented into different zones as per security requirements? Whether the organization has installed network security devices, such as WAF (web application firewall), proxy servers, IPS, etc. to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources. Has the organization implemented suitable monitoring tools to monitor the traffic within the organization's network and to and from the organizations network? Does the organization periodically conduct Network Architecture Security assessments in order to identify threats and vulnerabilities? Are the findings of such assessments tracked and closed? Are Internet facing servers placed in a DMZ and segregated from other zones by using a firewall? Is there segregation between application and database servers? Are user and server zones segregated? Are specific port/service accesses granted on firewall by following a proper approval process? Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/STWT/DMA?
8	**Access Controls**

Audit TOR Clause	TOR Details
8(a)	Access to server rooms – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.
8(b)	Additional Access controls – Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the CTCL/Non NEAT Frontend (NNF) terminals (CTCL/ NNF / IBT/ STWT / ALGO / DMA / SOR) respectively. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.
8(c)	Access Control Does the organization's documented policy and procedure include the access control policy? Is access to the information assets based on the user's roles and responsibilities? Does the system have a password mechanism which restricts access to authenticated users? Does the system request for identification and new password before login into the system? Does the system have appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager? Does the organization ensure that access control between website hosting servers and internal networks is maintained? Are records of all accesses requested, approved, granted, terminated and changed maintained? Are all accesses granted reviewed periodically? Does the organization ensure that default system credentials are disabled/locked? Are Application development, Testing (QA and UAT) and Production environments segregated? Whether adequate controls have been implemented for admission of personnel into the server rooms / place where servers / hardware / systems are located and whether audit trails of all the entries/exits at the server room / location are maintained? Is access to the information assets based on the user's roles and responsibilities? Does the system have a password mechanism which restricts access to authenticated users?
8(d)	Extra Authentication Security If the systems uses additional authentication measures like smart cards, biometric authentication or tokens etc.
8(e)	Physical & Environmental Security Does the organization have a documented process/framework for Physical & Environmental Security? Are adequate provisions in respect of physical security of the hardware / systems at the hosting location and controls on admission of personnel into the location (audit trail of all entries-exits at location etc.)? Are security perimeters defined based on the criticality of assets and operations? Are

Audit TOR Clause	TOR Details
	periodic reviews conducted for the accesses granted to defined perimeters? Are CCTV cameras deployed for monitoring activities in critical areas? Is the CCTV footage backed up and can it be made available in case the need arises? Are suitable controls deployed for combating fire in Data Center? Does the organization maintain physical access controls for · Server Room/Network Room security (environmental controls) Server Room .Network Room Security (UPS), Server room. network room security (HVAC) Are records maintained for the access granted to defined perimeters? Are suitable controls deployed for combating fire in the data center?
8(f)	Privileged Identity Management Does the organization have a documented process/procedure for defining reviewing and assigning the administrative roles and privileges? Has the organization implemented controls/tools for Privilege Identity Management including at a minimum provisioning, maintenance, monitoring, auditing and reporting all the activities performed by privileged users (Sys Admin, DBA etc.) accessing organization's IT systems? Are Privileges granted to users based on appropriate approvals and in accordance with the user's role and responsibilities? Are all the activities of the privileged users logged? Are log reviews of privileged user logs of admin activity conducted periodically? Is Maker- Checker functionality implemented for all changes by admin? Are records of privileged user provisioning/deprovisioning reviewed?
8(g)	Closed User Group Endpoint Security 1- Does the ASP have policies and procedures having coverage related to People, Processes and Technology? 2- Does the ASP vendor have architecture that supports segregation such as Business - Other business of ASP Vendor, Data and Processing facilities, Development / Test / Production environment Corporate user and Production / server zones, Application and Database servers, Internet facing servers placed in a DMZ and segregated from other zones. Ensure appropriately configured firewalls are used to ensure segregation wherever needed. 3- Are technology related Baseline Controls established, exercised, and reviewed periodically 4- are following systems and processes existing and exercised for Vulnerability Assessment and Penetration Testing, Configuration of Technologies prior to go live, Monitoring of perimeter / network security, infrastructure and applications for anomalies alerts incidents and breaches Reporting of cyber-attacks, threats, cyber-incidents and breaches experienced and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats to be submitted to stock exchange and other regulatory agencies based on applicability.

Audit TOR Clause	TOR Details
8(h)	The active log-in session through IBT & STWT platforms be logged-out at the time of End-of-Day processing (EOD)/at defined time and subsequent login by clients/investors should only be permitted after successful Two-Factor Authentication (2FA) via OTP/M-Pin/T-Pin as per the Exchange circular no. NSE/COMP/68635
9	**Backup and Recovery**
9(a)	Backup and Recovery Policy – Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.
9(b)	Log generation and data consistency - Whether backup logs are maintained and backup data is tested for consistency.
9(c)	System Redundancy – Whether there are appropriate backups in case of failures of any critical system components.
9(d)	Backup & Restoration The Installed systems backup capability is adequate as per the requirements of the Exchange for overcoming loss of product integrity. Are backups of the following system generated files maintained as per the Exchange guidelines? At the server/gateway level a) Database b) Audit Trails Reports At the user level a) Market Watch b) Logs c) History d) Reports e) Audit Trails f)Alert logs Does the organization ensure that the audit trail data maintained is available for a minimum period of 5 years? Are backup procedures documented and backup logs maintained? Are the backup logs maintained and are the backups been verified and tested? Are the backup media stored safely in line with the risk involved? Are there any recovery procedures and have the same been tested? Are the backups restored and tested periodically to ensure adequacy of backup process and successful restoration?
9(e)	Audit trail, Event logging and monitoring o ASP should maintain logs of all trading activity to facilitate audit trail. o Whether system generates, captures and maintains audit trail of all transactions for at least 3 years? o All events, changes in master, strategy parameters shall be logged and maintained for at least 3 years. o Whether all logs generated are secured from unauthorized modifications?

Audit TOR Clause	TOR Details
9(f)	How will the organization assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location - Network / Communication Link Backup Is the backup network link adequate in case of failure of the primary link to the Exchange? Is the backup network link adequate in case of failure of the primary link connecting the users? Is there an alternate communications path between customers and the firm? Is there an alternate communications path between the firm and its employees? Is there an alternate communications path with critical business constituents, banks and regulators? Whether detailed network diagram is prepared and available for verification? Is network and network diagram in line with the one submitted to the Exchange? Does the organization have an alternate means of communication including channel for communication for communicating with the clients in case of any disruption. Such communication should be completed within 30 minutes from the time of disruption.
9(g)	How will the organization assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location - System Failure Backup Are there suitable backups for failure of any of the critical system components like a) Gateway / Database Server b) Router c) Network Switch Infrastructure breakdown backup Are there suitable arrangements made for the breakdown in any infrastructure components like d) Power Supply e) Water f) Air Conditioning

Audit TOR Clause	TOR Details
	Primary Site Unavailability Have any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery Are there suitable provisions for Books and records backup and recovery (hard copy and electronic). Have all mission-critical systems been identified and provision for backup for such systems been made?
10	**BCP/DR**
10(a)	BCP / DR Policy – Whether the ASP Vendor has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response Exchange procedures and observation on the DR drills conducted by the ASP Vendor. Further, the system auditor should verify whether specified ASPs have conducted DR Drills/ live trading from DR site on half yearly basis and whether all the clients were shifted to the DR site during the drill including running of all operations from DR site for at least 1 full trading day. The system auditor shall verify whether learning of DR drill has been documented including RTO and RPO?
10(b)	Alternate channel of communication – Whether the ASP Vendor has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).
10(c)	High Availability – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/DR policy.
10(d)	Connectivity with other FMIs – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.
10(e)	Business Continuity Does the Organisation have a suitable documented Business Continuity or Disaster Recovery or Incident Response process commensurate with the organization size and risk profile to ensure a high degree of availability of the installed system Is there any documentation on Business Continuity / Disaster Recovery / Incident Response? If a BCP/DRP plan exists, has it been tested on regular basis? Are there any documented risk assessments? Does the installation have a Call List for emergencies maintained?

Audit TOR Clause	TOR Details
	Whether redundancy is built at all level of infrastructure? Whether all critical systems / infrastructure are in HA mode?
10(f)	Security Incident & Event Management Does the organization have a documented process/policy for Security Incident & Event Management? Does the organization has a documented process/procedure for identifying Security related incidents by monitoring logs generated by various IT assets such as Operating Systems, Databases, Network Devices, etc.? Are all events/incidents detected, classified, investigated and resolved? Are periodic reports published for various identified Security incidents? Does the organization ensure that the logging facilities and the log information Are protected from tampering and unauthorized access?
10(g)	Security Incident & Event Management Is there a dedicated Incident Response Team for managing risk and compliance activities?
10(h)	Business Continuity Does the organization have a Disaster Recovery Site? Are there any documented risk assessments? Does the installation have a Call List for emergencies maintained? Does the organization have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients?
10(i)	1. The system auditor should comment on the documented incident response procedures. which will cover the following: a. Identification of all critical operations of the ASP and also include the process of informing clients in case of any disruptions. While putting in place the BCP/DR plan, ASPs are advised to sufficiently review all potential risks along with its impact on the business. b. Declaration of incident as a “Disaster” viz. timelines etc. and restoration of operations from DR Site upon declaration of ‘Disaster’ Adequate resources (with appropriate training and experience) should be available at the DR Site to handle all operations during disasters. c. The declaration of disaster shall be reported in the preliminary report submitted to the Exchange.

Audit TOR Clause	TOR Details
10(j)	1. Does the organisation have distinct primary and disaster recovery sites (DRS) for technology infrastructure, workspace for people and operational processes? Does the organisation have DRS set up sufficiently away (not less than 250 km), from Primary Data Centre (PDC) to ensure that both DRS and PDC are not affected by the same disasters? 2.Have any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery? Does the organisation have suitable provisions for Books and records backup and recovery (hard copy and electronic)? Have all mission-critical systems been identified and provision for backup for such systems been made?
11	**Segregation of Data and Processing facilities**
11(a)	The system auditor should check and comment on the segregation of data and processing facilities at the ASP Vendor in case the ASP Vendor is also running other business.
12	**Back office data**
12(a)	Data consistency – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.
12(b)	Trail Logs – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.
13	**User Management**
13(a)	User Management Policy – The system auditor should check whether the ASP Vendor has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.
13(b)	Access to Authorized users – The system auditor should check whether the system allows access only to the authorized users of the CTCL/ Non NEAT Frontend (NNF) System. Whether there is a proper documentation of the authorized users in the form of User Application approval, copies of User Qualification and other necessary documents.
13(c)	User Creation / Deletion – The system auditor should check whether new user ids were created / deleted as per Non NEAT Frontend (NNF) guidelines of the exchange and whether the user ids are unique in nature.
13(d)	User Disablement – The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log and trade logs of the user) are maintained.

Audit TOR Clause	TOR Details
13(e)	User Management system: User Deletion: Users are deleted as per the Exchange guidelines Reissue of User Ids: User Ids are reissued as per the Exchange guidelines. Locked User Accounts: Users whose accounts are locked are unlocked only after documented unlocking requests are made and deactivate dormant account/users.
13(f)	Is there any process to control the installation of approved software on endpoints. Has ASP implemented measures to control usage of VBA/macros in office documents, control permissible attachment types in email systems.
14	**IT Infrastructure Management (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))**
14(a)	IT Governance and Policy – The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed.
14(b)	IT Infrastructure Planning – The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.
14(c)	IT Infrastructure Availability (SLA Parameters) – The system auditor should verify whether the ASP firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the ASP Vendor firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the ASP firm
14(d)	IT Performance Monitoring (SLA Monitoring) – The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the ASP Vendor.
14(e)	Infrastructure High Availability - Does the organization have a documented process for identifying single point of failure? - Does the organization have a documented process for failover? - Does the organization ensure that various components pertaining to networks, servers, storage have sufficient redundancy? - Does the organization conduct periodic redundancy/contingency testing?

Audit TOR Clause	TOR Details
14(f)	To ensure information security for the Organization in general and the installed system in particular policy and procedures as per the Exchange requirements must be established, implemented and maintained. Does the organization's documented policy and procedures include the following policies and if so are they in line with the Exchange requirements and whether they have been implemented by the organization? Information Security Policy Password Policy User Management and Access Control Policy Network Security Policy Application Software Policy Change Management Policy Backup Policy BCP/DR Management Policy Audit Trail Policy Capacity Management Plan Patch Management Policy Does the organization follow any other policy or procedures or documented practices that are relevant?
14(g)	Are documented practices available for various system processes Day Begins Day Ends Other system processes a) Audit Trails b) Access Logs c) Transaction Logs d) Backup Logs e) Alert Logs f) Activity Logs g) Retention Period h) Data Maintenance
14(h)	In case of failure, is there an escalation procedure implemented? Day Begin Day End Other system processes Details of the various response procedures including for a) Access Control failure b) Day Begin failure

Audit TOR Clause	TOR Details
	c) Day End failure d) Other system Processes failure
14(i)	Vulnerability Assessment, Penetration Testing & Application Security Assessments: Are periodic vulnerability assessments for all the critical assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS etc conducted?
14(j)	Standards & Guidelines Does the organization maintain standards and guidelines for information security related controls, applicable to various IT functions such as System Administration, Database Administration, Network, Application, and Middleware etc.? Does the organization maintain Hardening Standards pertaining to all the technologies deployed within the organization related to Applications, OS, Hardware, Software, Middleware, Database, Network Devices and Desktops? Does the organization have a process for deploying OS, Hardware, Software, Middleware, Database, Network Devices and Desktops after ensuring that they are free from vulnerabilities? Are the defined standards, guidelines updated and reviewed periodically?
14(k)	Information Security Policy & Procedure - Does the organization's documented policy and procedures include the information security policy and if so are they compliant with legal and regulatory requirements? Are the defined policies & procedures reviewed on a periodic basis?
14(l)	Information Security Policy & Procedure Are any other standards/guidelines like ISO 27001 etc. being followed? Does the organization have an Information Security Forum to provide overall direction to information security initiatives based on business objectives?
14(m)	Information Classification & Protection: Has the organization defined Systematic and documented framework for Information Classification & Protection? Are the information items classified and protected in accordance with business criticality and sensitivity in terms of Confidentiality, Integrity & Availability? Does the organization conduct periodic information classification process audits? Has the organization deployed suitable controls to prevent leakage of sensitive information?
14(n)	Vulnerability Assessment, Penetration Testing & Application Security Assessments Does the organization maintain an annual VAPT and Application Security Assessment activity calendar? Is periodic Router ACL review conducted as a part of Vulnerability Assessment?
14(o)	Does the organisation have hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
14(p)	Amazons AWS S3 and EC2 service Controls: Does the organization check public accessibility of all AWS instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations?

Audit TOR Clause	TOR Details
14(q)	Does the organization ensure proper security of AWS access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc. ?
14(r)	Does the organisation implement appropriate security measures for production, testing, staging and backup environments hosted on AWS? Does the organization ensure that production environment is kept properly segregated from these? Does the organisation disable/remove older or testing environments if their usage is no longer required?
14(s)	The Apache Software Foundation released an emergency patch as part of the 2.15.0 release of Log4j that fixes the Remote Code Execution (RCE) vulnerability. Does the Organizations verify the use of the latest and stable version of Log4j package in their environment or any third parties component engaged with them through scanning and patching of such vulnerabilities?
14(t)	Has the ASP Vendor obtained and maintained valid SOC-II compliance reports from all third-party vendors providing virtual assets (e.g., cloud services such as SaaS, PaaS, IaaS)?
15	**Software Testing Procedures - The system auditor should check whether the ASP vendor has complied with the guidelines and instructions of Stock exchanges with regard to testing software and new patches, including the following:**
15(a)	Test Procedure Review – The system auditor should review and evaluate the procedures for system and software/program testing. The system auditor should also review the adequacy of tests.
15(b)	Documentation – The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organizations standards.
15(c)	Test Cases – The system auditor should review the internal test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange and various SEBI circulars.
16	**Additional Points**
16(a)	Antivirus Management Does the organization have a documented process/procedure for Antivirus Management? Are all information assets protected with anti-virus software and the latest anti-virus signature updates? Does the organization periodically performs scans for virus/malicious code on computing resources, email, internet and other traffic at the Network Gateway/entry points in the IT Infrastructure? Does the organization have a documented process/procedure for tracking, reporting and responding to virus related incidents?

Audit TOR Clause	TOR Details
16(b)	Anti-virus Is a malicious code protection system implemented? If Yes, then Are the definition files up-to-date? Any instances of infection? Last date of virus check of entire system
16(c)	The installed system provides a system based event logging and system monitoring facility which monitors and logs all activities / events arising from actions taken on the gateway / database server, authorized user terminal and transactions processed for clients or otherwise and the same is not susceptible to manipulation. The installed systems has a provision for On-line surveillance and risk management as per the requirements of Exchange and includes Number of Users Logged In / hooked on to the network incl. privileges of each The installed systems has a provision for off line monitoring and risk management as per the requirements of Exchange and includes reports / logs on a) Number of Authorized Users b) Activity logs c) Systems logs d) Number of active clients
16(d)	Firewall Whether suitable firewalls are implemented? Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT systems
16(e)	Compliance Does the organization have a documented process/policy implemented to ensure compliance with legal, statutory, regulatory and contractual obligations and avoid compliance breaches? Does the organization ensure compliance to the following? · IT Act 2000 · Sebi Requirement Does the organization maintain an integrated compliance checklist? Are these defined checklists periodically updated and reviewed to incorporate changes in rules, regulations or compliance requirements? Whether the order routing servers routing CTCL/IBT/STWT/orders are located in India. Provide address of the CTCL / IBT / STWT server location (as applicable)

Audit TOR Clause	TOR Details
	Whether the required details of all the Non NEAT Frontend (NNF) facility user ids created in the server of the ASP, for any purpose (viz. administration, branch administration, mini-administration, surveillance, risk management, trading, view only, testing, etc) and any changes therein, have been uploaded as per the requirement of the Exchange? If no, please give details. Whether all the CTCL/ Non NEAT Frontend (NNF) facility user ids created in the server of the ASP have been mapped to 12 digit codes on a one-to-one basis and a record of the same is maintained? If no, please give details. The system has an internal unique order numbering system. All orders generated by CTCL/ Non NEAT Frontend (NNF) terminals (CTCL/IBT/DMA/STWT/SOR/ALGO) are offered to the market for matching and system does not have any order matching function resulting into cross trades. Whether algorithm orders are having unique flag/ tag as specified by the Exchange. All orders generated from algorithmic system are tagged with a unique identifier – 13th digit of field is populated appropriately. Whether every algorithm order reaching on exchange platform is tagged with the unique identifier allotted to the respective algorithm by the Exchange. All orders routed through CTCL/IBT/STWT/DMA/SOR/ALGO are routed through electronic / automated Risk Management System of the ASP to carry out appropriate validations of all risk parameters before the orders are released to the Exchange. The system and system records with respect to Risk Controls are maintained as prescribed by the Exchange which are as follows : · The limits are setup after assessing the risks of the corresponding user ID and branch ID · The limits are setup after taking into account the member's capital adequacy requirements · All the limits are reviewed regularly and the limits in the system are up to date · All the branch or user have got limits defined and that No user or branch in the system is having unlimited limits on the above stated parameters · Daily record of these limits is preserved and shall be produced before the Exchange as and when the information is called for · Compliance officer of the member has certified the above in the quarterly compliance certificate submitted to the Exchange IBT/STWT Compliance: Does the ASP's IBT / STWT system complies with the following provisions : · The system captures the IP (Internet Protocol) address (from where the orders are originating), for all IBT/ STWT orders

Audit TOR Clause	TOR Details
	· The system has built-in high system availability to address any single point failure · The system has secure end-to-end encryption for all data transmission between the client and the ASP system through a Secure Standardized Protocol. A procedure of mutual authentication between the client and the ASP server is implemented · The system has adequate safety features to ensure it is not susceptible to internal/ external attacks · In case of failure of IBT/ STWT, the alternate channel of communication has adequate capabilities for client identification and authentication · Two-factor authentication for login session has been implemented for all orders emanating using Internet Protocol · In case of no activity by the client, the system provides for automatic trading session logout · The back-up and restore systems implemented by the ASP is adequate to deliver sustained performance and high availability. The ASP system has on-site as well as remote site back-up capabilities · Name of the website provided in the application form is the website through which Internet based trading services is to be provided to the clients. · Secured socket level security for server access through Internet is available. · SSL certificate is valid and ASP is the owner of the website provided. Any change in name of the website or ownership of the website shall be incorporated only on approval from the Exchange - Whether the order routing servers routing CTCL/ALGO/IBT/WT/DMA/orders are located in India and through specified CTCL / ATS User ID approved by the Exchange for Trading - ATF software / IDs do not have any interlink with any system or ID located / linked outside India. - Whether the required details of all the CTCL/NNF user ids created in the server of the ASP, for any purpose (viz. administration, branch administration, mini-administration, surveillance, risk management, trading, view only, testing, etc.) and any changes therein, have been uploaded as per the requirement of the Exchange? If no, please give details. - Whether all the CTCL/NNF user ids created in the server of the ASP have been mapped to 12 digit codes on a one-to-one basis and a record of the same is maintained? If no, please give details.

Audit TOR Clause	TOR Details
	- The system has an internal unique order numbering system. - All orders generated by CTCL/ Non NEAT Frontend (NNF) terminals (CTCL/IBT/WT/ALGO/DMA/SOR) are offered to the market for matching and system does not have any order matching function resulting into cross trades. - All orders routed through CTCL / IBT / WT / DMA / are routed through electronic / automated Risk Management System of the ASP to carry out appropriate validations of all risk parameters before the orders are released to the Exchange.
16(f)	Vendor Certified Network diagram Date of submission of network diagram to Exchange(Only in case of change in network setup, ASP needs to submit revised scanned copy network diagram along with this report) Verify number of nodes in diagram with actual Verify location(s) of nodes in the network
16(g)	DOS Has the organization implemented strong monitoring, logging, detection and analysis capability to detect and mitigate DOS/DDOS attacks? Does the organization have a documented process/procedure/policy defining roles and responsibilities and plan of action in order to deal with DOS/DDOS attacks pro-actively and post the incidence?
16(h)	DOS Does the organization periodically conduct mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks?
16(i)	Third Party Information Security Management Does the organization have a documented process/framework for Third Party Vendor Management including at a minimum process and procedure for on-boarding/off-boarding of vendors, checklist for prescribing and assessing compliance, assessment and audit for both onsite & offsite vendors? Does the organization conducts periodic information security compliance audits/reviews for both onsite and offsite vendors? Are Risks associated with employing third party vendors addressed and mitigated? Is the defined process/framework periodically reviewed?

Audit TOR Clause	TOR Details
16(j)	Capacity Management • Does the organization have documented processes/procedures for capacity management for all the IT assets? • Are installed systems & procedures adequate to handle algorithm orders/trades? • Is there a capacity plan for growth in place? System auditor shall verify whether the ASP has put in place, a mechanism to handle increase in capacity in proportion to the increase in client base/financial turnover. • Are System bandwidth utilization and throughput being monitored, tracked and reported periodically? • Whether peak load is monitored for all critical systems and alerts generated on threshold reaching 70% of capacity • Is there a mechanism to track triggered alerts and issues resolved timely.
16(k)	Independent Audits Are periodic independent audits conducted by Third Party / internal Auditors? Are the audit findings tracked to closure?
16(l)	Human Resources Security, Acceptable Usage & Awareness Trainings Are periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors? Has the organization implemented policy/procedure defining appropriate use of information assets provided to employees and vendors in order to protect these assets from inappropriate use? Are these policies/procedures periodically reviewed and updated? Does the organization perform Background Checks for employees (permanent, temporary) before employment? Does the organization conduct Information Security Awareness Program through trainings and Quiz for employees and vendors?
16(m)	Does the organization display the 'Risk disclosures' given at Annexure-I Circular no SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/73 dated May 19, 2023 on their websites and to all their clients in the manner as specified below: 1. Upon login into their trading accounts with ASP Vendors, the clients may be prompted to read the 'Risk disclosures' (which may appear as a pop-up window upon login) and shall be allowed to proceed ahead only after acknowledging the same. 2. The 'Risk disclosures' shall be displayed prominently, covering at least 50 percent area of the screen.
16(n)	Whether a functionality is developed on ASP Vendor's (with retail clients) non-NEAT front end including IBT,STWT,CTCL etc whereby any person placing an order in a security which is under Graded Surveillance Measure(GSM)/ Additional Surveillance Measure(ASM)/IRP as per IBC/Unsolicited SMS or Videos/Pledge/ASM ICA/ASM IBC etc gets the message as per Exchange circular NSE/SURV/55831 dated March 1,

Audit TOR Clause	TOR Details
	2023, at the time of placing the order and is aware of such surveillance action on the scrip before placing the order.
16(o)	Compliance with circular NSE/SURV/ 64402 dated October 04, 2024 [read along with Circular nos. NSE/SURV/64924 dated November 06, 2024, and NSE/SURV/ 65097 dated November 14, 2024]. Whether the Member/ASP has developed the functionality to facilitate dissemination of scrip specific cautionary messages (single/multiple) on trading terminals at the time of order entry to identify securities which are under Surveillance and Other actions, on their non-NEAT front end including IBT, STWT, CTCL etc., as per Exchange Circular nos. NSE/SURV/54513 dated Nov 18, 2022, NSE/SURV/57778 dated July 31, 2023, NSE/SURV/60281 dated January 16, 2024 & NSE/SURV/ 64402 dated October 04, 2024. Whether any person (client of the Member) while placing an order in a security for which the cautionary indicators are applicable (as per the REG1_INDDDMMYY.csv file and 'fo_secban_DDMMYYYY.csv'), gets the cautionary alert message so that the person placing the order is aware of such single/multiple actions on the scrip before placing the order. In case multiple messages are eligible to be displayed, whether ASPs are providing all eligible messages in the pop-up. Whether the Member/ASP has included the verbatim of the pop-up message as per the Exchange Circular dated October 4, 2024 [read along with Circular nos. NSE/SURV/64924 dated November 06, 2024 and NSE/SURV/ 65097 dated November 14, 2024] on the trading front-end. Whether the Member/ASP has maintained a LOG of all such displays per scrip and the options (Yes or No) selected by the investor on the order entry screen. Whether Management of the TM has provided such LOGs to the Board of the ASP and satisfied them that all alerts were displayed at the time of order entry and the option chosen by the client on the system was also recorded. Whether the System Auditor has checked in the periodic submission, whether the above functionality was properly deployed.
16(p)	Whether the ASP is complying with the Exchange circular NSE/INSP/55031 dated December 28, 2022 for "Display of ASP brokerage, Statutory & Regulatory Levies"
16(q)	Whether member is allowing to place orders to only approved FPI clients using DMA facility as specified in as per SEBI/HO/MRD/MRD-RAC-1/P/CIR/2022/131

Audit TOR Clause	TOR Details
	September 29, 2022 regarding Participation of SEBI registered Foreign Portfolio Investors(FPIs)in Exchange Traded Commodity Derivatives in India and SEBI circular i.e. SEBI/HO/MRD/MRD-PoD-1/P/CIR/2023/68 May 10, 2023 regarding "Direct Market Access(DMA)to SEBI registered Foreign Portfolio Investors (FPIs) for participating in Exchange Traded Commodity Derivatives(ETCDs)"
17	**AI-ML**
17(a)	Are adequate safeguards in place to prevent abnormal behavior of the AI or ML application / System.
17(b)	Has Algo enabled members and other trading members/ASP reported details of AI/ML to Exchange on a half yearly and annual basis respectively, in accordance with SEBI circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019, and Exchange circular number - NSE/COMP/59700 dated 12 December 2023.
17(c)	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report.
18	**Undertaking/Application for CTCL/IBT/STWT/DMA/SOR**
18(a)	The system has been installed after complying with the various Exchanges circulars issued from time to time Copy of Undertaking provided regarding the CTCL system as per relevant circulars. Copy of application for approval of Internet Trading, if any. Copy of application for approval of Securities trading using Wireless Technology, if any Copy of application for approval of Direct Market Access, if any. Copy of application / undertaking provided for approval of Smart Order Routing (SOR)
19	**Pre Trade Risk Control**
19(a)	Whether appropriate pre-trade checks, alerts, and controls are built in Non-NEAT Frontend (NNF) facility/ systems such that an alert shall be generated if the user places limit order at a price which is away from prevailing market prices.
20	**Asset Management**
20(a)	Does the organization have a documented process/framework for managing all the hardware & software assets? Does the organization maintain a centralized asset repository? Are periodic reconciliation audits conducted for all the hardware and software assets to confirm compliance to licensing requirements and asset inventory? Has the ASP maintained list of approved/ authorised software? Whether the IT asset inventory contains the information regarding the hostname, IP Address, Asset Owner, Operating System details, Criticality of asset, Asset Tagging, end-of-life/ end-of-support, last patched date, etc. Whether the mitigating / compensatory controls mentioned in Risk Register are

Audit TOR Clause	TOR Details
	adequate to address the risks emanating from End of Life or End of Support Software / Systems? Whether the installed Software Versions and License are reviewed and Risk related to Software has been addressed in Risk Register?
21	**Phishing & Malware Protection for IBT / STWT**
21(a)	Has the organization implemented controls/ mechanism to identify and respond to phishing attempts on their critical websites? Are the organizations websites monitored for Phishing & Malware attacks? Does the organization have a process for tracking down phishing sites?
22	**Smart order routing (SOR) - The system auditor should check whether proper procedures have been followed, and proper documentation has been maintained for the following:**
22(a)	a. Best Execution Policy – System adheres to the Best Execution Policy while routing the orders to the exchange. b. Destination Neutral – The system routes orders to the recognized stock exchanges in a neutral manner. c. Class Neutral – The system provides for all classes of investors d. Confidentiality - The system does not release orders to venues other than the recognized stock Exchange. e. Opt–out – The system provides functionality to the client who has availed of the facility, to specify for individual orders for which the clients do not want to route order f. Time stamped market information – The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail facility. g. Audit Trail - Audit trail for should capture order details, trades and data points used as a basis for routing decision. h. Server Location : The system auditor should check whether the order routing server is located in India i. Alternate Mode - The system auditor should check whether an alternative mode of trading is available in case of failure of Facility
23	**Remote Access Controls**
23(a)	Does the organization have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources are securely located in the data center from home, using internet connection?
23(b)	For implementation of the concept of trusted machine as end users: Does the organization have categorized the machines as official desktops / laptops and accordingly the same are configured to ensure implementation of solution stack considering the requirements of authorized access?

Audit TOR Clause	TOR Details
23(c)	Does the organization's official devices have appropriate security measures to ensure that the configuration is not tampered with. Does the organization ensure that internet connectivity provided on all official are not getting used for any purpose other than the use of remote access to data center resources?
23(d)	Does the organization ensure that if personal devices (BYOD) are allowed for general functions, then appropriate guidelines are issued to indicate positive and negative list of applications that are permitted on such devices? Further, are these devices subject to periodic audit?
23(e)	Does the organization implement various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility.? VPN remote access through MFA also needs be implemented.
23(f)	Does the organization ensure that only trusted machines are permitted to access the data center resources? Does the organizations Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures?
23(g)	Does the organization have appropriate risk mitigation mechanisms whenever remote access of data center resources is permitted for service providers?
23(h)	For on-site monitoring, the ASP, Does the organization implement adequate safeguard mechanisms such as cameras, security guards, nearby co- workers to reinforce technological activities?
23(i)	Does the organizations backup, restore and archival functions work seamlessly, particularly if the users have remote access to internal systems.?
23(j)	Does the organization apply only necessary and applicable patches to the existing hardware and software?
23(k)	Does the organization analyse generated alerts and alarms? And take appropriate decisions to address the security concerns? Are the organizations security controls for the Remote Access requirements integrated with the SOC Engine and part of the overall monitoring of the security posture?
23(l)	Does the organization have updated the incident response plan in view of the current pandemic? Does the plan cover following : 1.Increase awareness of information technology support mechanisms for employees who work remotely. 2.Implement cyber security advisories received from SEBI, Exchange, CERT-IN and NCIIPC on a regular basis. 3.Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness. 4.Disable use of Macros in Microsoft office

Audit TOR Clause	TOR Details
24	**SEBI and Exchange Compliances**
24(a)	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges and mention
24(b)	1- Adherence to all such Circulars, Notices, Guidelines, and advisories published
24(c)	2- Reporting adherences based on prescribed periodicity in point 1 above
24(d)	Has ASP taken corrective steps to rectify the deficiencies observed in the inspection carried out by SEBI? Further, whether ASP has complied with the qualifications/violations made in last SEBI inspection report?
24(e)	Has Member/ASP taken corrective steps to rectify the deficiencies observed in the inspection carried out by Exchange? Further, has Member/ ASP complied with the qualifications/violations made in last Exchange inspection report?

Annexure G

Terms of Reference (TOR) applicable for Cyber Audit

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
1	**Governance**	
1(a)	GV.RR.S3	Has the ASP Vendor designated a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/Partners/Proprietor of the ASP Vendor? Is the reporting of the CISO directly to the MD & CEO of their organization? Does the CISO possess sufficient qualification and capabilities to carry out his/her responsibilities? Has the ASP Vendor established a reporting procedure to facilitate communication of cybersecurity incidents/unusual activities to the CISO or to the senior management in a time-bound manner as defined by guidelines/policies/laws/circulars/regulations, etc.? Is the level, grade, and standing of the CISO at least equivalent to CTO/CIO?
1(a)(i)	GV.RR.S3	Has the ASP vendor appointed a senior official or management personnel (the 'Designated Officer') responsible for assessing, identifying, and reducing cybersecurity risks; responding to incidents; establishing appropriate standards and controls; and directing the development and implementation of processes and procedures in line with the cybersecurity and cyber resilience policy approved by the Board, Partners, or Proprietor? Has the ASP vendor implemented a reporting procedure to communicate cybersecurity incidents/unusual activities to the Designated Officer within a time-bound framework, in compliance with SEBI or GoI guidelines, policies, laws, circulars, or regulations?
1(b)	GV.RR.S4	Has the ASP vendor allocated an adequate percentage of the total IT budget to cybersecurity? Has this allocation been mentioned under a

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		separate budgetary head for monitoring by the Board of Directors or top-level management?
1(b)(i)	GV.RR.S4	Has the ASP vendor ensured that adequate resources are allocated and aligned with the cybersecurity risk strategy, roles and responsibilities, and policies? Whether the resources are defined in terms of budgetary allocation, people, and material, and are resourcing requirements revisited regularly based upon progress or shortfalls in the implementation of standards and reflected in the budgetary allocation?
1(c)	GV.RR.S5, GV.RR.S6	Has the ASP vendor ensured that every employee hired, irrespective of the department or role, presents a low/no threat to the ASP vendors' cybersecurity posture by following the below steps? 1. Conducting due diligence 2. Ensuring employees receive proper security training during onboarding and on a regular basis 3. Following employment screening procedures, employment policies and agreements, employment termination procedures, etc.?
1(d)	GV.RR.S6	Has the ASP vendor signed a confidentiality and integrity agreement with third-party service providers and conducted due diligence of all third-party service providers accessing their IT systems?
1(e)(i)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has the ASP vendor formulated a comprehensive Cybersecurity and Cyber Resilience policy document encompassing CSCRF as part of the operational risk management framework to manage risks to systems, networks and databases from cyber-attacks and threats,?
1(e)(ii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document?
1(e)(iii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has the policy document been approved by the Board / Partners / Proprietor of the ASP vendor? Is the policy document reviewed by the aforementioned group periodically with a view to strengthen and improve cyber resilience posture?
1(e)(iv)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework?
1(e)(v)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the Policy Approval Date is captured in the respective policy

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
1(e)(vi)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has policy version maintained for all the policy/procedure documents
1(e)(vii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the policy is approval is captured in policy/procedure documents
1(e)(viii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	1.Does the ASP vendor have policies (including but not limited to) with respect to asset management, patch management, vulnerability management, VAPT policy, audit policy, monitoring of the networks and endpoints, configuration management, change management, secure software development life cycle management, authentication policies, authorization policies and processes, network segmentation/isolation policies, commissioning internet-facing assets, encryption policies, PII and privacy policies, cybersecurity control management policy, asset ownership documentation, etc., and a chain of command for any approval process in the organization with respect to cybersecurity? 2.Do the policies contain do's and don'ts in the organization with respect to the usage of information assets including desktops, laptops, BYOD, networks, internet, data, etc. as a part of the ASP vendor's cybersecurity policy or as standalone policies? The aforementioned policies may form a part of ASP vendor's cybersecurity policy or may be standalone policies.
1(e)(ix)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Does the Cybersecurity Policy include the following process to identify, assess, and manage cybersecurity risks associated with processes, information, networks, and systems: 1. Identify critical IT assets and risks associated with such assets. 2. Protect assets by deploying suitable controls, tools, and measures. 3. Detect incidents, anomalies, and attacks through appropriate monitoring tools/processes. 4. Respond by taking immediate steps after identification of the incident, anomaly, or attack. 5. Recover from the incident through incident management and other appropriate recovery mechanisms?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
1(e)(x)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Does the organization follow the Plan-Do-Check-Act concept while creating and using documented information, where activities under the 'Plan' phase are guided by Policies, the 'Do' phase follows Procedures (SOPs), and the 'Check' and 'Act' phases refer to the Policies and Procedures?
1(e)(xi)	GV.PO.S1, GV.PO.S2, GV.PO.S5	As part of compliance management with respect to CSCRF, Whether the ASP vendor has applied the following key aspects (including but not limited to) for implementing compliance management: 1. Assess Compliance with applicable guidelines / policies / laws / circulars / regulations, etc., issued by SEBI or GoI. 2. Develop compliance policies and procedures 3. Implement controls such as security measures 4. Train employees 5. Monitor and review compliance management processes 6. Regular audits and reporting. while the Auditor must list all applicable implementations of Circulars, Notices, Guidelines, and advisories published by CERT-In, CSIRT-Fin Advisories, SEBI, and Exchanges/Depositories.
1(e)(xii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the Board/Partners/Proprietor of the ASP has constituted an IT Committee for ASP vendors comprising experts proficient in technology? Does this IT Committee of ASP vendors meet on a periodic basis to review the implementation of the cybersecurity and cyber resilience policy approved by their Board/Partners/Proprietor, and does such review include goal setting for a target level of cyber resilience, and establishing a plan to improve and strengthen cybersecurity and cyber resilience? Is the review placed before the Board/Partners/Proprietor of the ASP vendor for appropriate action?
1(e)(xiii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Does the aforementioned committee and the senior management of the ASP vendor, including the CISO, periodically review instances of cybersecurity incidents/attacks, if any, domestically and globally, and take steps to strengthen cybersecurity and cyber resilience?
1(e)(xiv)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the ASP vendor has incorporated best practices from standards such as ISO 27001, ISO 27002, etc., or their subsequent revisions, if any, from time to time?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
1(f)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether policy document have considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.
1(g)	GV.OC.S2, GV.OC.S3	Does the ASP vendor define and document roles and responsibilities of its employees, outsourced staff, and employees of vendors, or participants and other entities, who may have privileged access or use systems/networks of the ASP Vendor towards ensuring the goal of cybersecurity?
1(h)	GV.OV.S4	Whether the ASP has conducted self-assessments of its cyber resilience using CCI and submit corresponding evidence to its submission authority annually? Is CCI and its calculation methodology done as outlined in (Annexure-K) of SEBI CSCRF? Whether the RE has strived to build an automated tool and suitable dashboards (preferably integrated with a log aggregator) for submitting compliance of CCI? Is a dashboard available at the time of cyber audit, onsite inspection/audit by SEBI or any agency appointed by SEBI?
1(i)	PR.IP.S1	Has the ASP vendor ensured that IT, OT, and IS infrastructure is 'secure by design', 'secure by engineering/ implementation', and that the infrastructure has appropriate elements to ensure 'secure IT operations'?
1(j)	PR.IP.S4, PR.IP.S6	Before introducing new technologies for critical systems, has the ASP vendor ensured that the IT/security team has assessed evolving security concerns and achieved a fair level of maturity with such technologies before incorporating them into IT infrastructure?
1(k)	PR.MA.S3	Is the procurement of hardware/software aligned with the technology refresh policy of the ASP vendor?
1(l)	RS.MA.S1	Has the ASP vendor formulated an up-to-date CCMP in line with the national CCMP of CERT-In?
1(l)(i)	RS.MA.S1	Has the CCMP been approved by the Board/Partners/Proprietor of the ASP vendor?
1(m)	RS.IM.S2	Have the updates and changes in the contingency plan, COOP, training exercises, and incident response and recovery plan been communicated and approved by the Board/Partners/Proprietor?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
1(n)	RC.CO.S1, RC.CO.S2, RC.CO.S3	Has the ASP vendor discussed recovery plans with the IT Committee for ASP vendors? Do the plans include stakeholders' coordination in the recovery process, and both internal and external communication?
1(o)	PR.IP.S3	Is the change management process part of all agreements with third-party service providers to ensure that changes to the system are implemented in a controlled and coordinated manner?
1(o)(i)	PR.IP.S3	Does the Change Management process include (but not limited to) submission, planning (impact analysis, rollout plan), approval, implementation, review (post-implementation), closure, etc.?
1(o)(ii)	PR.IP.S3	Does the ASP vendor have a clearly defined framework for change management including requirements justifying exception(s), duration of exception(s), the process of granting exception(s), and authority for approving and for periodic review of exception(s) given?
1(p)	PR.IP.S14	Periodic Audit 1.Has the ASP vendor engaged only CERT-In empanelled IS auditing organizations for conducting external audits, including cyber audits, to audit the implementation of all standards mentioned in this framework? 2.Has the CERT-In empanelled IS auditing organization been changed after three consecutive years? 3.Along with the cyber audit reports, has the ASP vendor also submitted a declaration from the Managing Director (MD)/Chief Executive Officer (CEO) as mentioned in Annexure B of SEBI CSCRF dated August 20, 2024? 4.Does the audit management process of the ASP vendor include (but not limited to) audit program/calendar, planning, preparation, delivery, evaluation, reporting, and follow-up, etc.? 5.For conducting audits, are CERT-In 'IT Security Auditing Guidelines for Auditee Organizations' followed by the ASP vendor? Additionally, are CERT-In 'Guidelines for CERT-In Empanelled IS Auditing Organizations' (as outlined SEBI CSCRF) mandated for empanelled IS auditing organizations? 6.Is due diligence with respect to the audit process and the tools used for such audits undertaken by ASP to ensure the competence and effectiveness of audits?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
1(q)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor proactively assess and take necessary actions with respect to its system's requirements, architecture, design, configuration, acquisition processes, or operational processes as a strategy for adaptation to the identified and prospective threats and vulnerabilities?
1(q)(i)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor strive to rapidly deploy and integrate existing and new services, both on-premises and in the cloud?
1(r)	PR.IP.S17	Does the ASP vendor follow the latest version of CIS Controls or equivalent standards, which are prioritized sets of safeguards and actions for cyber defense and provide specific and actionable ways to mitigate prevalent cybersecurity incidents/attacks?
1(s)	PR.MA.S3	Has the ASP vendor established a patch management policy to ensure that all applicable patches (at both PDC and DR Site) are identified, assessed, tested, and applied to all IT systems/applications in a timely manner? Has the policy been approved by the IT Committee for ASP vendors? Additionally, is the above-mentioned policy on patch management reviewed by the IT Committee for ASP vendors on an annual basis?
1(t)	DE.DP.S4	The results of the red teaming exercise been placed before the IT Committee for ASP vendors and the Governing board? Is the status of the remediation of the observations found during the red team exercise monitored by the IT Committee for ASP vendors?
1(u)	RS.CO.S2	Does the IT Committee for ASP vendors discuss response plans, coordination with stakeholders for consistency in response actions, information sharing for better awareness, etc.?
1(v)	RC.RP.S2	Have the results of the Cyber resilience testing been placed before the IT Committee for ASP?
2	**Identification**	
2(a)	GV.SC.S5	Has the ASP vendor obtained SBOM for their existing critical systems within 6 months (starting from the date of applicability of SEBI CSCRF)?
2(a)(i)	GV.SC.S5	Has the ASP vendor obtained SBOMs for any new critical systems software products/Software-as-a-Service applications (SaaS) at the time of procurement? Do SBOMs containing information such as all the open source and third-party components present in a codebase, versions of the components used in the codebase, and their patch

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		status, etc., allow security teams to quickly identify any associated security or license risk?
2(a)(ii)	GV.SC.S5	Whether the SBOM obtained has included (but not limited to) the following? 1. License information 2. Name of the supplier 3. All primary (top level) components with all their transitive dependencies (including third-party dependencies whether in-house or open-source components) and relationships 4. Encryption used 5. Access control 6. Cryptographic hash of the components 7. Frequency of updates 8. Known unknown (where a SBOM does not include a full dependency graph) 9. Methods for accommodating occasional incidental errors 10. All software/ applications required for core and critical business operations (irrespective of in-house or third-party) shall have a SBOM which documents all (but not limited to) components, dependencies, data relationships, etc.
2(a)(iii)	GV.SC.S5	Are Software Bill of Materials (SBOM) regularly reviewed for open-source and third-party components, with documented risk assessments and update processes in place?
2(b)	ID.AM.S1, ID.AM.S4	Has the ASP vendor identified and classified critical systems as defined in the SEBI CSCRF framework based on their sensitivity and criticality for business operations, services, and data management? Is the list of critical systems approved by the Board/Partners/Proprietor of the ASP vendor?
2(b)(i)	ID.AM.S1, ID.AM.S4	Has the ASP vendor maintained an up-to-date inventory of their (including but not limited to) hardware and systems, software, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets), interfacing systems (internal and external), details of its network resources, connections to its network, and data flows?
2(b)(ii)	ID.AM.S1, ID.AM.S4	Has any additions/deletions or changes in existing assets reflected in the asset inventory within 3 working days?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
2(b)(iii)	ID.AM.S1, ID.AM.S4	For conducting criticality assessment of assets, Whether the ASP vendor has taken the following steps (including but not limited to): 1. Maintain a comprehensive asset inventory 2. Conduct threat modelling (based on risk assessment) 3. Conduct vulnerability assessment
2(c)	ID.RA.S1, ID.RA.S2	Risk Management: Does the ASP vendor conduct a risk assessment in consultation with their IT committee (including post-quantum risks) of the IT environment of their organization on a yearly basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture? Is the aforementioned risk assessment utilized by the ASP vendor to develop a quantifiable cybersecurity risk score?
2(c)(i)	ID.RA.S1, ID.RA.S2	Has the ASP vendor accordingly identified cyber risks that they may face, along with the likelihood of associated threats and their impact on their business, and deployed controls commensurate to their criticality?
2(c)(ii)	ID.RA.S1, ID.RA.S2	Does Risk Assessment include (but not limited to): 1. Technology stack and solutions used 2. Known vulnerabilities 3. Dependence on third-party service providers 4. Data storage, security and privacy protection 5. Threats, likelihoods and associated risks
2(d)	ID.AM.S6	Are all IT assets inventoried in the ITSM tool? Has the ASP vendor integrated cybersecurity considerations into product life cycles?
2(e)	PR.AA.S6	Is an effective authentication policy implemented with the defined complexity of the password? Are all generic user IDs and email IDs which are not in use removed after the use?
3	**Protection**	
3(a)	GV.SC.S5	Whether encryption is used? Whether access control is in place?
3(b)	PR.AA.S6	Has the ASP vendor implemented strong password controls for users' access to systems, applications, networks, and databases, etc.? Do password controls include (but not limited to) a change of password upon first login, minimum password length and history, password complexity as well as maximum validity period? Is the user credential data stored using strong hashing algorithms?
3(c)	PR.AT.S3	Does ASP provide access to mobile and web applications to a customer only at her/ his option based on specific written or authenticated

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		electronic requisition along with a positive acknowledgement of the terms and conditions?
4	**Risk Management**	
4(a)	GV.RM.S1, GV.RM.S2	A) Whether the design of the cyber risk management framework has considered the following (including but not limited to): 1. Identification of the cybersecurity risk for the organization 2. Classification of identified and mapped business functions, supporting processes, and information assets at risk. 3. Determination of risk appetite for IT and cybersecurity risks. 4. Definition of mitigation measures and controls to reduce the risks. 5. Monitoring of the effectiveness of the above-mentioned measures and controls. 6. Evaluation of the effect of major changes and significant operational, technical, or cybersecurity incident(s) on the risks? B) Whether the ASP vendor has used the latest version of ISO 27005 as a guidance on design, implementation, and maintenance of information security risk management? C) Does the risk management strategy of the ASP vendor include (but not limited to) risk assessment, risk analysis, risk mitigation, risk monitoring and review, compliance with relevant laws and regulations, communication of risk management policies to all stakeholders, effective mitigation measures with options for compensatory controls wherever feasible, measures to reduce residual risk and ensuring that the cybersecurity risk tolerance is within acceptable limits?
4(a)(i)	GV.RM.S1, GV.RM.S2	1.Does the ASP vendor utilize metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), the number of cybersecurity incidents/intrusion attempts detected and resolved within a specific period, the number of false positives and false negatives generated by cybersecurity monitoring tools, the number of successful cyber attacks in the past year, and the measures taken to reduce these numbers through continuous refinement of the monitoring process to assess their cybersecurity maturity level? 2.Does the ASP vendor periodically assess the level of employee cybersecurity awareness, for e.g., through phishing test success rates, etc.?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		3.Does the ASP vendor undertake periodic IT asset management for functions such as the number of devices on the network running end-of-life (EOL) software, the number of devices no longer receiving security updates, unidentified devices on the internal network, the integration of third-party devices and services into the network, etc.? Further, is IT asset management also utilized for the process of managing assets' access and permissions, patching cadence, security rating, third-party security rating, the number of known vulnerabilities, etc.? 4. Is a risk-based transaction monitoring or surveillance process implemented as part of the fraud risk management system across all delivery channels?
4(b)	GV.RM.S3	1. Is comprehensive scenario-based testing conducted to assess the cybersecurity risks of the ASP vendor? ASP vendors shall prepare their own attack scenarios as per their business model and assess their risks accordingly.
4(c)	ID.RA.S4	1. Is a risk assessment of authentication-based solutions conducted to gain insights into the context behind each login attempt? Additionally, does the risk-based authentication solution analyze factors such as device, location, network, and sensitivity when a user attempts to sign in?
5	**Physical Security**	
5(a)	PR.AA.S10, PR.AA.S11, PR.AA.S12	Physical Security 1. Is physical access to critical systems restricted to a minimum and provided only to authorized officials? 2. Is physical access provided to third-party service providers properly supervised by ensuring that third-party service providers are accompanied at all times by authorized employees? 3. Are employees of the ASP screened before being granted access to organizational information and information systems? 4.Is physical access to critical systems revoked immediately when it is no longer required? 5.Has the ASP ensured that the perimeter of the critical equipment rooms, if any, is physically secured and monitored by employing physical, human, and procedural controls such as security guards, CCTVs, card access systems, mantraps, bollards, etc., wherever appropriate?
6	**Access Control**	

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
6(a)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1.Does any person, by virtue of rank or position have any intrinsic right to access confidential data applications, system resources, or facilities? 2.Is access to ASP vendor systems, applications, networks, and databases granted for a defined purpose and period? 3.Is access to IT systems, applications, databases, and networks granted on a need-to-use basis and based on the principle of least privilege? Are such access provided for a specific duration using effective authentication mechanisms? 4.Are user access rights, delegated access, unused tokens, and privileged users' activities reviewed periodically? 5. Is access to external cloud services such as Dropbox, Google Drive, iCloud, OneDrive, etc., given as per ASP vendor's policy? 6.Are account access lock policies implemented for all accounts after a certain number of failed login attempts? 7.Are existing user accounts and access rights periodically reviewed by the system owner to detect dormant accounts, accounts with excessive privileges, unknown accounts, or any discrepancies? 8.Are proper 'end of life' mechanisms adopted for user management to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn? Does this include named user IDs, default user IDs, and generic email IDs?
6(a)(i)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1.Is Privileged Identity Management (PIM) solution or process implemented to monitor and manage privileged access? 2. Does ASP vendor implement an access policy that includes strong password controls for users' access to systems, applications, networks, and databases? 3. ASP vendors shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT infrastructure of ASP vendors. 4. Does ASP vendor deploy controls and security measure ASP vendor to supervise staff with elevated system access entitlements (such as admin or privileged users)?Do such controls and measure ASP vendor include Restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.? Do ASP vendor

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users)?Do such controls and measures include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.?
6(b)	PR.AA.S4, PR.AA.S5	1. Does the ASP vendors have implemented suggested strategies/ methodologies such as Zero-trust networks, segmentation, no single point of failure, high availability, etc. and the same have been approved by IT committee for ASP vendors? 2. Are delegated access and unused tokens reviewed and cleaned at least on a quarterly basis?
6(c)	PR.AA.S16, PR.AA.S17	Is access management, including effective authentication and authorization, implemented to ensure that only the authorized ASP vendor can access the APIs?
6(c)(i)	PR.AA.S16, PR.AA.S17	Does the mobile application undergo re-authentication whenever the device remains unused for a designated period and each time the investor/user launches the application?
6(d)	PR.MA.S2	Has ASP vendors ensured a proper remote access policy framework that incorporates the specific requirements for securely accessing enterprise resources (located in the data center) from home using an internet connection?
7	**Network Security Management**	
7(a)	ID.AM.S1, ID.AM.S4	Has the ASP vendor prepared and maintained an up-to-date network architecture diagram at the organizational level including wired and wireless networks?
7(b)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1. Do all critical systems accessible over the internet have multi-factor security measures (such as VPNs, firewall controls, etc.) and multi-factor authentication (MFA)? 2.Is MFA enabled for all users and systems that connect using online/internet facilities, particularly for VPNs, webmail, and accounts that access critical systems from non-trusted environments to trusted environments?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
7(b)(i)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	**Network Security Management** 1. Are adequate controls deployed to address virus, malware, and ransomware attacks on servers and other IT systems? Do these controls include host/network/application-based Intrusion Prevention Systems (IPS), customized kernels for Linux, anti-virus, and anti-malware software? Are anti-virus definition file updates and automatic anti-virus scanning performed regularly? 2. Has the ASP vendor established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, enterprise mobile devices, etc., within the IT environment? Does the ASP vendor also conduct regular enforcement checks to ensure that baseline standards are applied uniformly? 3. Are the LAN and wireless networks within the organization's premises secured with proper access controls? 4.Does the ASP vendor limit the total and maximum connections to the SMTP server?
7(b)(ii)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	Network Security Management 1. Has the ASP applied appropriate network segmentation and isolation techniques to restrict access to sensitive information, hosts, and services? Is segment-to-segment access based on a strong access control policy and the principle of least privilege? 2. Has the ASP installed network security devices, such as Web Application Firewalls (WAF), proxy servers, and Intrusion Prevention Systems (IPS), to protect their IT infrastructure exposed to the internet from security threats originating from internal and external sources? 3. Has the ASP deployed web and email filters on the network? Are these devices configured to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages, filter out emails with known malicious indicators (such as known malicious subject lines), and block suspicious IP addresses and malicious domains/URLs at the firewall? Are all emails, attachments, and downloads scanned with a reputable antivirus solution both on the host and at the mail gateway?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		4. Are network devices configured in line with the whitelist approach of IPs, ports, and services for inbound and outbound communication with proper Access Control List (ACL) implementation? 5. Has the ASP implemented DNS filtering services to ensure only clean DNS traffic is allowed in the environment? Is DNS security extension used for secure communication? Is the management of critical servers, applications, services, and network elements restricted through enterprise-identified intranet systems? 6. Has the ASP implemented Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting & Conformance (DMARC), and DomainKeys Identified Mail (DKIM) for email security? 7. Does email protection include best practices such as strong password protection, multi-factor authentication (MFA), spam filtering, email encryption, a secure email gateway, and permissible attachment types? 8. Has the ASP blocked malicious domains and IPs after diligent verification without impacting operations? Are CSIRT-Fin/CERT-In advisories, which are published periodically, referred to for the latest malicious domains, IPs, Command & Control (C&C) DNS, and links? 9. Does the ASP maintain an up-to-date and centralized inventory of authorized devices connected to their network (both within and outside the ASP premises) and authorized devices enabling the network? Does the ASP implement solutions to automate network discovery and management?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
7(c)	PR.AA.S10, PR.AA.S11, PR.AA.S12	**Remote Support Service Security** 1. As many OEMs and their service partners, as well as System Integrators, provide remote support services to organizations, does the ASP vendor ensure that these services are well-governed, controlled, logged, and that oversight is maintained on all the activities done by remote support service providers? Are the above complemented by regular monitoring and audit to ensure compliance with the defined policies for privileged users and remote access? 2. Does the ASP vendor ensure secure usage of RDP in IT systems? Is it implemented strictly on a need-to-use basis and does it employ MFA? Is remote access, if necessary, given to authorized personnel from whitelisted IPs for a predefined time period, with a provision to log all activities? 3. Are employees and third-party service providers who may be given authorized access to the critical systems, networks, and other IT resources of ASP vendors subject to stringent supervision, monitoring, and access restrictions?
7(d)	PR.AA.S15	**Endpoint security** 1. Are solutions like Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and anti-malware software implemented to detect threats and attacks on endpoint devices, and to enable immediate response to such threats and attacks? Does the ASP vendor ensure that signatures are updated on all IT systems? 2. Are solutions like Intrusion Prevention Systems (IPS) and Next-Generation Intrusion Prevention Systems (NG-IPS) used to continuously monitor the organization's network for malicious activities?
7(e)	PR.AA.S16, PR.AA.S17	Has ASP vendor ensured connection to entities via APIs being strictly based on a whitelist approach?
7(e)(i)	PR.AA.S16, PR.AA.S17	1.Does the mobile application check new network connections or connections for unsecured networks like VPN connections, proxy, and unsecured Wi-Fi connections?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
7(f)	PR.IP.S1	1. Is the practice of whitelisting ports based on business usage implemented at the firewall level, rather than blacklisting certain ports? Is traffic on all other ports that have not been whitelisted blocked by default? 2. Does the ASP vendor utilize host-based firewalls to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communications among endpoints wherever possible to limit lateral movement and other attack activities?
7(g)	5(k)	1. Is the Network Time Protocol (NTP) server configured to be synchronised with National Physical Laboratory (NPL) or National Informatics Centre (NIC) or any associated servers for synchronisation of all ICT system clocks? As per circular NSE/INSP/67637
7(h)	PR.MA.S2	1. Does the ASP ensure that only trusted client machines are permitted to access enterprise IT resources remotely? Has the RE put in place appropriate security control measures such as (including but not limited to) host integrity check, binding of the MAC address of the device with the IP address, etc., for remote access and telecommuting? Has the RE ensured that appropriate risk mitigation mechanisms are put in place whenever remote access of data center resources is permitted for third-party service providers?
8	**Data security**	
8(a)	PR.DS.S4	Does the ASP vendor enforce effective data protection, backup, and recovery measures?
8(a)(i)	PR.DS.S4	Has the ASP vendor implemented measures to control the usage of VBA/macros in office documents and control permissible attachment types in email systems?
8(a)(ii)	PR.DS.S4	Does the ASP vendor have a documented data migration policy specifying SOPs and processes for data migration while ensuring data integrity, completeness, and consistency?
8(b)	PR.AA.S15	**Restricted Use of Removable Media and Electronic Devices** 1.Has the ASP vendor defined and implemented a policy for restriction and secure use of removable media (such as USB, external hard disks, etc.) and electronic devices (such as laptops, mobile devices, etc.)? 2. Does the ASP vendor ensure secure erasure of data so that no data is in recoverable form on such media and electronic devices after use?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
8(c)	PR.AA.S16, PR.AA.S17	1.Does the mobile application store/retain sensitive personal/investor authentication information such as user IDs, passwords, keys, hashes, hardcoded references, etc., on the device? Does the application securely wipe out any sensitive investor/user information from memory when the investor/user exits the application?
8(d)	PR.DS.S1, PR.DS.S2, PR.DS.S3	**Data and Storage Devices Security** 1.Is data encrypted in motion, at rest, and in-use by using strong encryption methods? 2. Whether data-in-use encryption for cloud deployments as per reference mentioned in Annexure J of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** is followed or not? 3. Is layering of Full-disk Encryption (FDE) along with File-based Encryption (FBE) used wherever possible? 4. Does the ASP vendor use industry-standard, strong encryption algorithms (e.g., RSA, AES, etc.) wherever encryption is implemented? 5. Are the illustrative measures given in Annexure-H and Annexure-I of CSCRF circular been provided for data security on customer-facing applications and data transport security being implemented? 6. Have Data Loss Prevention (DLP) solutions or processes been deployed by the ASP vendor? 7.Has the ASP vendor implemented measures to prevent unauthorized access, copying, and transmission of data/information held in contractual or fiduciary capacity? 8. Does the ASP vendor ensure that the confidentiality of information is not compromised during the process of exchanging and transferring information with external parties? 9.Are the illustrative measures been provided in data transport security to ensure the security of data during internet transmission being implemented? 10. Does the information security policy cover the use of devices such as mobile phones, photocopiers, scanners, etc., which can be used for capturing and transmission of sensitive data within their IT infrastructure? 11.Are access policies for personnel and network connectivity for such devices defined?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		12. Does the ASP vendor allow only authorized data storage devices within their IT infrastructure through appropriate validation processes?
9	**Hardening of Hardware and Software**	
9(a)	PR.DS.S4	Does the ASP vendor block administrative rights on end-user workstations/PCs/laptops by default and provide access rights on a need basis as per the established process and approvals and for the specific duration for which it is required?
9(b)	PR.IP.S1	Does the implementation of the principle of least functionality include measures such as configuring only essential capabilities by disabling unnecessary and/or unsecured functions, ports, protocols, services, etc., within the information system?
9(b)(i)	PR.IP.S1	**Hardening of Hardware and Software** 1.Does the ASP vendor deploy only hardened and vetted hardware/software? During the hardening process, does the ASP vendor, inter-alia, ensure that default usernames and passwords are replaced with non-standard usernames and strong passwords, and all unnecessary services are removed or disabled in software/systems? 2. Has OS hardening been done to protect servers'/endpoints' OS and minimize attack surface and exposure to threats? 3.Does the ASP vendor ensure that for running services, non-default ports are used wherever applicable? Has the ASP vendor blocked open ports on networks and systems that are not in use or could potentially be exploited? Does the ASP vendor monitor all open ports and take appropriate measures to secure them? 4.Has the ASP vendor restricted the execution of "PowerShell" and "wscript" in their environment, if not required? Additionally, has the ASP vendor installed the latest version of PowerShell, with enhanced logging enabled, script block logging, and transcription enabled? Are the associated logs being sent to a centralized log repository for monitoring and analysis?
9(b)(ii)	PR.IP.S1	Does the ASP vendor use application directory whitelisting on all assets to ensure that only authorized software is run and all unauthorized software is blocked from installation/execution?
9(c)	PR.AA.S15	Are the PowerShell and local admin rights disabled by default on endpoint machines and used only for a specific purpose and for a limited time?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
9(d)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor strive to reduce their attack surfaces?
9(d)(i)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor look for the feasibility of deploying diverse operating systems? Would an attack or compromise on one type of OS affect other OSs deployed?
10	**Application Security in Customer Facing Applications**	
10(a)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has the ASP vendor formulated a policy for mobile and web applications and associated services with the approval of their Board/Partners/Proprietor? Do the contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/mitigation measures, compliance with regulatory instructions, customer experience, etc., explicitly include security requirements from Functionality, Security, and Performance (FSP) angles?
10(b)	PR.AT.S3	Has the ASP vendor mentioned/incorporated a section on the mobile and web application clearly specifying the process and procedure (with forms/contact information, etc.) to lodge customer/investor grievances with respect to technology-related issues and cybersecurity? Has a mechanism been put in place to keep this information periodically updated? Does the reporting facility on the application provide an option for registering a grievance? Is customers'/investors' dispute handling, reporting, and resolution procedure, including the expected timelines for response, clearly defined?
10(b)(i)	PR.AT.S3	Does ASP vendor mention/incorporate a section on the mobile and web application clearly specifying the process and procedure (with forms/contact information, etc.) to lodge customer/investor grievances with respect to technology-related issues and cybersecurity? Is a mechanism in place to keep this information periodically updated? Does the reporting facility on the application provide an option for registering a grievance?
10(b)(ii)	PR.AT.S3	Does the ASP vendor provide a mechanism on their mobile and web application for their customers/investors with necessary authentication to identify/mark a transaction as fraudulent for seamless and immediate notification to his entities? On such notification by the customer/investor, do they endeavor to build the

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		capability for seamless/instant reporting of fraudulent transactions to the corresponding beneficiary/counterparty's entities; vice-versa have a mechanism to receive such fraudulent transactions reported from other entities?
10(c)	PR.DS.S4	Do the security controls for mobile and web applications focus on how these applications handle, store, and protect PII and other business-related data?
10(c)(i)	PR.DS.S4	Do web and mobile applications store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data?
10(d)	PR.IP.S4, PR.IP.S6	**Secure Software Development Cycle (SSDLC)** 1. Has the ASP vendor prepared business requirement documents with clear mentioning of security requirements, session management, audit trail, logging, data integrity, security event tracking, exception handling, etc.? 2. Has the ASP vendor conducted threat modelling and application security testing during the development phase for the secure rollout of software and applications? 3.Has the ASP vendor referred to standards, security guidelines for application security and other protection measures given by OWASP (for e.g., OWASP-ASVS)? 4.Has the ASP vendor adopted the principle of defence-in-depth to provide a layered security mechanism?
10(d)(i)	PR.IP.S4, PR.IP.S6	**Secure Software Development Life Cycle (SSDLC)** 1.Does the ASP vendor undertake regression testing before new or modified systems are implemented? 2. Does the scope of these tests cover business logic, security controls, system performance under various stress-load scenarios, and recovery conditions?
10(e)	PR.IP.S15	1. Are the tests/audits mentioned in point 1 (a-b) limited to cybersecurity aspects? Does application security testing also include API security and API discovery? 2. Does the scope of the functional audit cover data integrity, report integrity, and transaction integrity, etc.?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
10(f)	PR.AA.S16, PR.AA.S17	**API Security:** 1.Does the ASP vendor use effective API security strategies like rate limiting and throttling while developing APIs to prevent overuse or abuse? 2.Does the ASP vendor have API security solutions in place for securing services and data transmitted through APIs? 3.Does the ASP vendor follow OWASP documentation for developing APIs, and are OWASP top 10 API security risks mitigated? 4.Any entity connecting to ASP vendors via APIs, is that allowed to connect strictly on a whitelist-based approach? 5. Has the ASP vendor ensured compliance to Exchange circular NSE/INSP/62912 dated July 11, 2024?
10(f)(i)	PR.AA.S16, PR.AA.S17	1.Does the mobile application implement a device-binding solution to create a unique digital identity based on the device, mobile number, and SIM? 2. Is OWASP – MASVS referred for implementing mobile application security and other protection measures? 3.Has the ASP vendor implemented measures such as installing a "containerized" app on mobile/smartphones for exclusive business use that is encrypted and separated from other smartphone data/applications? Have measures been implemented to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement?
10(f)(ii)	PR.AA.S16, PR.AA.S17	Guidelines for Application Security and Emerging Technologies Has the ASP vendor prepared SOPs for open source application security and concerns from emerging technologies like Generative AI security?
10(g)	PR.DS.S1, PR.DS.S2, PR.DS.S3	**Application Security in Customer Facing Applications:** 1.Does the ASP vendor address application security for customer-facing applications offered over the Internet, such as IBTs (Internet-Based Trading applications), portals containing sensitive or private information, given their significant attack surfaces due to public availability? 2.Is the illustrative list of measures provided in Annexure G of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113**

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		dated August 20, 2024 for ensuring security in customer-facing applications under application authentication security being implemented?
10(h)	PR.DS.S5	Does the ASP vendor ensure that separate production and non-production environments are maintained for the development of all software/applications and feature enhancements?
10(h)(i)	PR.DS.S5	Does the ASP vendor conduct System Integration Testing (SIT) after development and/or feature enhancement to ensure that the complete software/application is working as required?
10(h)(ii)	PR.DS.S5	1. During the development phase of any software or application intended for use by ASP vendor or its customers, is it ensured that vulnerabilities identified by best practice baselines, such as OWASP Top 10 and SANS Top 25 software security vulnerabilities, are addressed? 2. Has the ASP vendor adopted methodologies such as DevSecOps to ensure the secure development of their applications and software?
11	**Patch management**	
11(a)	GV.SC.S5	1.Does the ASP vendor have a defined schedule for patch updates? How frequently are these updates applied to ensure the security and integrity of the software and systems?
11(b)	PR.DS.S4	Does the ASP vendor ensure that their digital certificates used in IT systems are renewed well in advance to prevent any lapses in security?
11(c)	PR.MA.S3	Has the ASP vendor established and ensured that the patch management procedures include the identification, categorization, and prioritization of patches and updates? Is an implementation timeframe for each category of patches established to apply them in a timely manner?
11(c)(i)	PR.MA.S3	1.Does the organization update all operating systems and applications with the latest patches on a regular basis? 2.Does the organization consider virtual patching as an interim measure for zero-day vulnerabilities when patches are not available? 3.Does the organization source patches only from the authorized sites of the OEM to ensure their authenticity and security?
11(c)(ii)	PR.MA.S3	1.Does the ASP vendor perform comprehensive and rigorous testing of security patches and updates, wherever possible, before deployment into the production environment to ensure that the application of patches does not impact other systems?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
11(c)(iii)	PR.MA.S3	Does the organization ensure that all patches are tested first in a non-production environment that closely resembles the production environment?
11(c)(iv)	PR.MA.S3	Does the organization ensure that hardware and software of critical systems are replaced before they reach End-of-Life or End-of-Support to maintain security and operational integrity?
11(c)(v)	PR.MA.S3	Does the organization implement compensatory controls, such as virtual patching, for legacy systems for a maximum period of 6 months? Does the organization ensure that the constraints necessitating virtual patching are legitimate and properly documented?
11(c)(vi)	PR.MA.S3	Does the ASP vendor ensure that post-application of any patch/update, the resources deployed are adequate enough to deliver the expected performance?
11(c)(vii)	PR.MA.S3	Does the ASP vendor have established processes for tracking patch compliance across all IT systems and applications, and are these compliance reports submitted to the respective IT Committee on a quarterly basis?
11(c)(viii)	PR.MA.S3	1. Does the ASP vendor ensure that patches are implemented at both PDC and DR sites within the following upper/maximum time limits based on their criticality: High: 1 week Moderate: 2 weeks Low: 1 month 2. For emergency patching, does the ASP vendor deploy patches within the timelines stipulated by the OEMs?
12	**Disposal of data, systems, and storage devices**	
12(a)	PR.AA.S13, PR.AA.S14	Has the ASP vendor formulated a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data?
12(a)(i)	PR.AA.S13, PR.AA.S14	Has the ASP vendor framed suitable policies for disposal of storage media and systems? Is the critical data/information on such devices and systems removed by using methods such as wiping/cleaning/overwrite, degauss/crypto shredding/physical destruction as applicable?
13	**Vulnerability Assessment and Penetration Testing (VAPT)**	

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
13(a)	ID.AM.S1, ID.AM.S4	1.Does the organization conduct threat modelling based on risk assessment to identify and mitigate potential vulnerabilities early in the software development lifecycle? 2.Does the organization conduct regular vulnerability assessments to identify, quantify, and prioritize security weaknesses in their systems and applications?
13(b)	PR.IP.S15	1.Does the ASP vendor ensure that all categories of software solutions, applications, and products for critical systems mandatorily pass through the following tests, audits, and compliances? 2.Does the ASP vendor conduct Dynamic Application Security Testing (DAST) to scan software applications in real-time against leading vulnerability sources, such as OWASP Top 10 and SANS Top 25 CWE, to identify security flaws or open vulnerabilities? 3.Does the ASP vendor conduct Static Application Security Testing (SAST) to analyze program source code and identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, and OWASP Top 10 security risks? 4.Does the ASP vendor conduct functional audits to verify that the software meets all specified requirements and functions correctly? 5.Does the ASP vendor conduct Vulnerability Assessment and Penetration Testing (VAPT) after every major release of the application or software to identify and address security weaknesses? 6.Does the ASP vendor integrate logs from all critical systems with the ASP vendor Security Operations Center (SOC) to ensure comprehensive monitoring and incident response? 7.Does the ASP vendor conduct audits of firewall configuration, Web Application Firewall (WAF) configuration, token configuration, and channel identification to ensure robust security settings? 8.Does the ASP vendor generate a Software Bill of Materials (SBOM) to provide a detailed inventory of all components used in the software, enhancing transparency and security? 9.Does the ASP vendor maintain a Requirement Traceability Matrix (RTM) to ensure that all requirements are tracked throughout the development lifecycle and are met?
13(c)(i)	DE.CM.S5	1.Does the ASP vendor regularly conduct cybersecurity audits and VAPT with the scope mentioned in CSCRF to detect vulnerabilities in the IT environment?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		2.Does the ASP vendor conduct in-depth evaluations of the security posture of the system through simulations of actual attacks? 3.An indicative (but not exhaustive and limited to) VAPT scope has been attached at Annexure-D of the circular.
13(c)(ii)	DE.CM.S5	Do the assets under these audits include (but not limited to) all critical systems, infrastructure components (like networking systems, security devices, load balancers, servers, databases, applications, remote access points, systems accessible through WAN, LAN as well as with Public IPs, websites, etc.), and other IT systems pertaining to the operations of ASP?
13(c)(iii)	DE.CM.S5	Does the ASP vendor perform VAPT prior to the commissioning of new systems, especially those which are part of critical systems or connected to critical systems?
13(c)(iv)	DE.CM.S5	Does the organization ensure that revalidation of VAPT is conducted in a time-bound manner post-closure of observations to confirm that all open vulnerabilities have been fixed??
13(d)	RS.AN.S4, RS.AN.S5	Does the ASP vendor conduct compromise assessments through CERT-In empanelled Information Security (IS) auditing organizations?
13(e)	PR.AA.S15	Guidance on Usage of Active Directory (AD) Servers 1.Does the ASP vendor regularly review the Active Directory (AD) to locate and close existing backdoors, such as compromised service accounts, which often have administrative privileges and are potential targets of attacks? 2.Does the ASP vendor undertake penetration testing activities for known AD Domain Controller abuse attacks? 3.Does the ASP vendor remediate identified weaknesses with the highest priority?
13(f)	DE.CM.S5	Does the ASP vendor ensure they engage only CERT-In empanelled organizations for conducting VAPT? Does the ASP vendor ensure that the final report on VAPT is submitted to the Exchange after approval from the Technology Committee of the respective ASP within one month of completion of the VAPT activity?
13(g)	PR.IP.S4, PR.IP.S6	For any production release, is vulnerability assessment undertaken? For all major releases, does the ASP vendor conduct a VAPT to assess the risks and vulnerabilities arising from recent additions or modifications in applications/software?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
13(h)	PR.IP.S14	Does the ASP vendor conduct revalidation VAPT and cyber audits in a time-bound manner to ensure that all open vulnerabilities in its IT assets have been fixed?
13(i)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor anticipate new attack vectors through threat modeling (based on risk assessment) and work to defend them?
13(j)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor proactively examine controls, practices, and capabilities for prospective, emerging, or potential threats?
13(j)(i)	DE.DP.S4	Does the ASP vendor conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis through the use of red/blue teams?
13(k)	DE.DP.S4	Does the ASP vendor deploy a CART solution for continuous, automated processing of testing the security of the systems and achieving greater visibility on attack surfaces?
13(k)(i)	DE.DP.S4	Does the red team for red teaming exercises consist of ASP vendor employees and/or outside experts? Additionally, is the red team independent of the function being tested?
14	**Monitoring and Detection**	
14(a)	ID.RA.S4	Measures against Phishing websites and attacks- Does the ASP vendor proactively monitor the cyberspace to identify phishing websites w.r.t. ASP vendor domains and report the same to CSIRT-Fin/CERT-In for taking appropriate action?
14(b)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1.Does the ASP vendor ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes? 2.Are such logs maintained and stored in a secure location for a time period not less than two (2) years (at least 6 months in online mode and the rest in archival mode)? 3.Does the ASP vendor also maintain records of users with access to shared accounts?
14(c)	PR.AA.S8	Does the ASP vendor ensure that all log sources are identified and their respective logs are collected? Additionally, does the ASP vendor collect an indicative list of log data types, including system logs, application logs, network logs, database logs, security logs, performance logs, audit trail logs, and event logs?
14(c)(i)	PR.AA.S8	Does the ASP vendor monitor all logs of events and incidents to identify unusual patterns and behaviors?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
14(d)	DE.CM.S1, DE.CM.S2, DE.CM.S3	Security Continuous Monitoring a.Has the ASP vendor established appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access, and unauthorized copying and transmission of data/information held in contractual or fiduciary capacity by internal and external parties? b.Does the ASP vendor monitor the security logs of systems, applications, and network devices exposed to the internet for anomalies? c.Does the ASP vendor generate suitable alerts in the event of detection of unauthorized or abnormal system activities, transmission errors, or unusual online transactions? d.To enhance security monitoring, does the ASP employ SOC services for their systems?
14(d)(i)	DE.CM.S1, DE.CM.S2, DE.CM.S3	Does the ASP utilizing third-party managed SOC services or market SOC obtain an SOC efficacy report from their SOC provider annually, using the quantifiable method outlined given Annexure N of SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024 from their SOC provider on a yearly basis?
14(d)(ii)	DE.CM.S1, DE.CM.S2, DE.CM.S3	Functional efficacy of SOC: Does the ASP assess the functional efficacy of their SOC using the quantifiable method as outlined in Annexure N of SEBI circular No. SEBI/HO/ ITD1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024? Does the ASP review the functional efficacy of SOC on a half-yearly basis? Does ASPs consider deploying a range of security solutions in consultation with their IT Committee, such as threat simulation, vulnerability management, and decoy systems, to assess and enhance their cybersecurity posture?
14(d)(iii)		The auditor shall verify that, ASP who have implemented/opted for Own / Group SOC (in accordance with SEBI CSCRF guidelines), are maintaining Functional efficacy of SOC & related reports as per guidelines and format provided in Annexure N of SEBI-CSCRF 2024.
14(e)	PR.AA.S10, PR.AA.S11, PR.AA.S12	Does the ASP vendor monitor environmental controls (temperature, water, smoke, etc.), service availability alerts (power supply, servers, etc.), and access logs?
14(f)	ID.RA.S3	Does the ASP vendor engage Dark web monitoring (for brand intelligence, customer protection, etc.), and takedown services as a

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		cyber-defence strategy to check for any brand abuse, data/credentials leak, combating cyber abuse, etc.?
14(f)(i)	ID.RA.S3	Does the ASP vendor have processes in place to manage and incorporate IOAs/ IOCs/ malware alerts/ vulnerability alerts (received from CERT-In or NCIIPC (as applicable) or any other government agencies) in their systems?
14(g)	PR.IP.S14	Does the ASP vendor strive to build an automated tool and suitable dashboards (preferably integrated with a log aggregator) for submitting compliance with CSCRF? Is a dashboard available at the time of cyber audit, onsite inspection/audit by SEBI or any agency appointed by SEBI?
14(h)	RS.AN.S1, RS.AN.S2, RS.AN.S3	Does the ASP vendor suitably investigate alerts generated from monitoring and detection systems to determine activities that should be performed to prevent the spread of cybersecurity incidents/attacks or breaches, mitigate their effects, and resolve the incidents?
14(i)	DE.CM.S4	Does ASP vendor ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet by implementing suitable mechanisms to monitor capacity utilization of its critical systems and networks, such as using firewalls to monitor bandwidth usage?
14(j)	PR.DS.S1, PR.DS.S2, PR.DS.S3	Does ASP vendor implement suitable mechanisms, including the generation of appropriate alerts, to monitor capacity utilization on a real-time basis and proactively address issues pertaining to their capacity needs? For capacity planning and monitoring, ASP vendors shall comply with circulars/ guidelines on capacity planning issued by SEBI & exchanges/Depositories (and updated from time to time).
14(k)	PR.MA.S2	Does the ASP vendor ensure that remote access is monitored continuously for any abnormal/unauthorized access, and appropriate alerts and alarms are generated to address this breach before any damage is done?
14(l)	DE.CM.S4	a.Is the use of IT assets/resources monitored, tuned, and are projections made for future capacity requirements to ensure the required system performance for meeting the business objectives? b.To ensure high resilience, high availability, and timely detection of attacks on systems and networks, does the ASP vendor implement suitable mechanisms to monitor capacity utilization of its critical systems and networks?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		Does the ASP vendor's capacity management comprise of three primary types; Data storage capacity – (e.g., in database systems, file storage areas, etc.), Processing power capacity – (e.g., adequate computational power to ensure timely processing operations), Communications capacity – ("bandwidth" to ensure communications are made in a timely manner). c.Is capacity management: Proactive – for example, using capacity considerations as part of change management? Reactive – e.g., triggers and alerts for when capacity usage is reaching a critical threshold so that timely increments (temporary or permanent) can be made?
14(m)	EV.ST.S1, EV.ST.S2, EV.ST.S3	6. Does the ASP vendor strive to rapidly correlate data using mathematical models and machine learning in order to make data-driven decisions?
14(m)(i)	EV.ST.S1, EV.ST.S2, EV.ST.S3	7. Does the ASP vendor use auditing/logging systems on different OS to acquire and store audit/logging data?
14(m)(ii)	EV.ST.S1, EV.ST.S2, EV.ST.S3	8. In order to include heterogeneity, are different audit/logging regimes applied at different architectural layers?
14(n)	DE.DP.S5	Does the ASP vendor proactively search for hidden and undetected cyber threats in their network?
14(o)	DE.DP.S5	Is threat hunting by leveraging threat intelligence, IOCs, IOAs, etc., conducted on a quarterly basis?
14(p)	DE.CM.S5	In case of vulnerabilities discovered in COTS (used for core business) or empanelled applications, does the ASP vendor report them to the vendors and the designated stock exchanges and/ or depositories in a timely manner?
15	**Response and Recovery**	
15(a)	GV.OC.S2	Does the ASP vendor engage a forensic auditor to identify the root cause of any incident (cybersecurity or other incidents) related to the ASP vendor?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
15(b)	RS.MA.S1	1.Has the ASP vendor developed an Incident Response Management Plan as part of their CCMP? 2.Does the response plan define responsibilities and actions to be performed by the ASP vendor employees and support/outsourced staff in the event of a cyberattack or cybersecurity incident? 3.Does the ASP vendor have an SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks? 4.Whether SOP as per Annexure -O of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** circular is adhered or not?
15(c)	RS.CO.S1, RS.CO.S2, RS.CO.S3	During the processing of reported incidents by SEBI, does the ASP vendor provide regular reports (such as RCA, forensic analysis report, etc.) on the progress of the incident analysis?
15(d)	RS.CO.S2	Does the ASP vendor notify the customer/investor, through alternate communication channels, of all transactions including buy/sell, payment or fund transfer above a specified value determined by the customer/investor?
15(d)(i)	RS.CO.S2	For the purpose of coordinating incident response, does the ASP vendor regularly update the contact details of service providers, intermediaries, and other stakeholders?
15(d)(ii)	RS.CO.S2	**If the cyberattack is of high impact and has a broad reach, does the ASP vendors had taken action as per their approved Cyber Crisis Management Plan (CCMP)?**
15(d)(iii)	RS.CO.S2	If the cyberattack is of low impact and has a narrow/low reach, does the ASP vendor inform all the affected customers/stakeholders?
15(e)	RS.AN.S1,RS.AN.S2, RS.AN.S3	Data collection: Does the ASP vendor collect and preserve data related to the incident, such as system logs, network traffic, and forensic images of affected systems?
15(e)(i)	RS.AN.S1, RS.AN.S2, RS.AN.S3	Incident Analysis: Does the ASP vendor analyze the data to understand the scope, cause, and impact of the incident, including how the incident occurred, what systems and data were affected, who was responsible, etc.?
15(e)(ii)	RS.AN.S1, RS.AN.S2, RS.AN.S3	Evidence Preservation: Does the ASP vendor preserve evidence related to the incident, including digital artifacts, network captures, and memory dumps, in a secure and forensically sound manner?
15(f)	RS.AN.S4, RS.AN.S5	Root Cause Analysis: Does the ASP vendor perform a root cause analysis (RCA) to identify the specific control that has failed, the

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		underlying cause of the incident, and the potential areas of improvement?
15(f)(i)	RS.AN.S4, RS.AN.S5	Forensic: Is forensic analysis (as appropriate) undertaken by the ASP vendor?
15(f)(ii)	RS.AN.S4, RS.AN.S5	Are incidents of loss or destruction of data or systems thoroughly analyzed, and are lessons learned from such incidents incorporated to strengthen the security mechanisms and improve the recovery planning and processes?
15(f)(iii)	RS.AN.S4, RS.AN.S5	Reporting: Does the ASP vendor create a detailed incident report that includes information on the scope, cause, and impact of the incident, as well as recommendations for improving incident response and recovery capabilities?
15(g)	RS.IM.S1	Does the ASP vendor periodically review and update their contingency plan, COOP, training exercises, and incident response and recovery plans (including CCMP) to incorporate lessons learned, and strengthen their response capabilities in the event of a future incident/attack?
15(g)(i)	RS.IM.S1	Post-occurrence of a cybersecurity incident (if any), does the ASP vendor update their response and recovery plan (including CCMP) to improve their cyber resilience and incorporate the learnings from the cybersecurity incident?
15(h)	RC.RP.S1	Do the response and recovery plans of the ASP vendor include scenario-based classifications? Does the ASP vendor build their own response and recovery plan as per their business model and include the same in their CCMP?
15(h)(i)	RC.RP.S1	Does the response and recovery plan of the ASP vendor include plans for the timely restoration of systems affected by cybersecurity incidents/attacks or breaches (for instance, offering alternate services or systems to customers)? Are tests designed to challenge the assumptions of response, resumption, and recovery practices, including governance arrangements and communication plans? Do these tests include all stakeholders such as critical service providers, vendors, other linked ASP vendors, etc.?
15(h)(ii)	RC.RP.S1	Is an indicative (but not exhaustive) recovery plan for the ASP vendor included in Annexure C of **of SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** followed or not?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
15(h)(iii)	RC.RP.S1	Has the ASP vendor maintain regularly updated "golden images" of critical systems at off-site locations for rebuilding the systems (whenever required)? Does this entail maintaining images “templates” that include a preconfigured operating system (OS), configuration setting backup, and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server?
15(h)(iv)	RC.RP.S1	Has the ASP vendor explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in an event that starting ASP vendor operations from PDC and/or DRS is not feasible? Does the ASP vendor also try to keep spare hardware in a ready-to-use state for delivering critical services, and are such systems updated as and when new changes (for example, OS patches, security patches, etc.) are implemented in the primary systems? Does this spare hardware regularly undergo testing in line with the response and recovery plan of the ASP vendor?
15(h)(v)	RC.RP.S1	Does Qualified ASP vendor has maintained spare hardware in ready-to-use state for delivering critical services, as it is mandated and as their business is critical to Indian securities market ecosystem?
15(h)(vi)	RC.RP.S1	Has the ASP vendor take all necessary precautions while updating the "golden" server images and data backup to ensure that server images and data backups are undamaged/unbroken?
15(h)(vii)	RC.RP.S1	In case of ransomware attacks that specifically target backups, does the ASP vendor create backups in an isolated and immutable (and/or air-gapped) manner to ensure recovery if the production system is compromised?
15(h)(viii)	RC.RP.S1	Has the ASP vendor undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level? Does the ASP vendor test recovering from a ransomware attack considering both PDC and DRS have been impacted to assess the effectiveness of people, processes, and technologies to deal with such attacks?
15(i)	RC.RP.S2	In the event of disruption of any one or more of the critical systems, Does the ASP vendors has designed and tested its systems and processes to enable the safe resumption of critical operations within two hours of a disruption, even in the case of extreme but plausible scenarios. Does the ASP vendors systems has capability to resume critical operations within two hours(i.e. RTO) and while dealing with a

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		disruption ASP vendors have exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate. In consultation with their IT Committee, Does the ASP vendors have also plan for scenarios in which the resumption objective is not achieved? Does ASP vendors have RPO of 15 minutes for critical systems as per SEBI Circular issued from time to time.
15(i)(i)	RC.RP.S2	Does the ASP vendor conduct comprehensive scenario-based cyber resilience testing at least 2 times in a financial year (periodicity of such testing shall be of 6 months), to validate their ability to recover and resume operations following a cybersecurity incident/attack within prescribed RTO and RPO defined by SEBI CSCRF? In this regard, does the ASP vendor incorporate extreme plausible cyberattack scenarios into their cyber response and recovery planning? Are the said scenarios devised by the ASP vendors in consultation with their respective IT Committee for ASP vendors based on the learning from various sources such as past cybersecurity incidents, near-miss analysis, data from Security Operations Centre, honeypot logs analysis, etc.?
15(i)(ii)	RC.RP.S2	Does the ASP vendor periodically conduct backup testing and restore back-up data to check its usability?
15(i)(iii)	RC.RP.S2	For cyber resilience testing, does the ASP also include stakeholders such as critical third-party service providers, market intermediaries, linked ASP vendors, etc.?
15(j)	RC.RP.S3	Does the ASP vendor conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan?
15(k)	RC.RP.S4	1.Has the ASP vendor formulated a backup and recovery plan approved by their respective IT Committee for ASP vendors? 2.Does the backup and recovery plan include policies and software solutions that work together to maintain business continuity in the event of a security incident? 3.Does such a plan include guidance on restoration of data with the backup software used by the ASP vendor?
15(k)(i)	RC.RP.S4	Does the backup and recovery policy include backup of data as well as backup of server images?
15(k)(ii)	RC.RP.S4	Are the backups of data and server images maintained at off-site locations to keep backup copies intact and unbroken?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
15(k)(iii)	RC.RP.S4	Are RTO and RPO, as prescribed by SEBI CSCRF from time to time, included in the recovery plan for the restoration of systems after cybersecurity incidents?
15(l)	RC.IM.S1	While ensuring the protection of data, and security of processes, do the ASP vendor's BCP-DR capabilities support its cyber resilience objectives, and rapid recovery and resumption of critical operations after a cybersecurity incident?
15(l)(i)	RC.IM.S1	Does the ASP vendor try to incorporate lessons learned from incidents reported (if any) by other ASP vendors?
15(m)	RC.IM.S2	Does the ASP vendor meet their RTO for all interconnected systems and networks through capacity upgradations and periodic coordinated resilience testing?
15(m)(i)	RC.IM.S2	Is the recovery plan improved after analyzing the learnings from periodic drills?
15(n)	RS.MA.S2	Does the ASP vendor prepare cyber playbooks? Has the ASP vendor created a knowledge database for all known adverse conditions and attacks?
15(o)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the ASP vendor maintain extra capacity of IT assets for information storage, processing, or communications?
15(p)	RC.RP.S4	Does the ASP vendor maintain offline, encrypted backups of data and regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity, and availability of data?
16	**Sharing of Information**	
16(a)	RS.CO.S1, RS.CO.S2, RS.CO.S3	Reporting of Cybersecurity Incidents Does the ASP vendor share Threat Intelligence data that is collected, processed, and analyzed to gain insights into the motives and behavior of the threat actor, target, attack pattern, etc.
16(a)(ii)	RS.CO.S1, RS.CO.S2, RS.CO.S3	Does the ASP vendor submit quarterly reports containing information on cyberattacks, threats, cybersecurity incidents, and breaches experienced, along with measures taken to mitigate vulnerabilities, threats, and attacks, including information on bugs/vulnerabilities and threats that may be useful for other ASP vendors and SEBI, within 15 days from the quarter ended June, September, December, and March of every year?
16(a)(iii)	RS.CO.S1, RS.CO.S2, RS.CO.S3	Does the ASP vendor share details deemed useful for other ASP vendors in a masked manner using a mechanism specified by SEBI from time to time? While sharing sensitive information, does the ASP

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		vendor follow TLP with four levels of sensitivity: white, green, amber, or red?
17	**Training and Education**	
17(a)	PR.AT.S1, PR.AT.S2	Does the ASP vendor work on building awareness of cybersecurity, cyber resilience, and system hygiene among employees (with a focus on employees from non-technical disciplines)?
17(a)(i)	PR.AT.S1, PR.AT.S2	Does the ASP vendor ensure that their employees are aware of potential risks including social engineering attacks, phishing, etc.?
17(a)(ii)	PR.AT.S1, PR.AT.S2	Has the ASP vendor established thoughtfully designed security awareness campaigns as an essential pillar of defense, stressing the avoidance of clicking on links and attachments in emails? Additionally, does ASP vendor refer to advisories issued by CERT-In/CSIRT-Fin for assistance in conducting exercises for public awareness?
17(a)(iii)	PR.AT.S1, PR.AT.S2	Does the ASP vendor conduct periodic training programs to enhance the knowledge of IT/cybersecurity policy and standards among employees, incorporating up-to-date cybersecurity threats? Where possible, is this extended to outsourced staff, third-party service providers, etc.?
17(a)(iv)	PR.AT.S1, PR.AT.S2	Does the ASP vendor review and update training programs to ensure that the contents remain current and relevant?
17(b)	RS.MA.S2	In order to optimize the ASP vendor's ability to respond in a timely and appropriate manner, Does the ASP vendor create cybersecurity awareness? Does the ASP vendor provide cybersecurity training to the relevant teams? Does the ASP vendor develop or hire people with appropriate skill sets?
17(c)	ID.RA.S3	Has the ASP vendor subscribed to anti-phishing/anti-rogue app services to mitigate potential phishing or impersonation attacks?
18	**Systems managed by vendors**	
18(a)	GV.SC.S4	Where the systems (IBT, Back office and other customer facing applications, IT infrastructure, etc.) of a ASP are managed by third-party service providers and in case the ASP does not have direct control over the implementation of any of the guidelines, whether the ASP has instructed the third-party service providers to adhere to the applicable guidelines in the CSCRF and has obtained the necessary cyber audit certifications from them to ensure compliance with the framework?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
18(a)(i)	GV.SC.S4	Does the responsibility, accountability, and ownership of outsourced activities lie primarily with the ASP vendor? Does the ASP vendor come up with appropriate monitoring mechanisms through a clearly defined framework to ensure that all the requirements as specified in SEBI CSCRF shall be complied with? Do the periodic reports submitted to SEBI highlight the critical activities handled by the third-party service providers, and does the ASP vendor certify that the above-mentioned requirement is complied with?
18(a)(ii)	GV.SC.S4	Does the ASP vendor conduct background checks and ensure signing of Non-Disclosure Agreements and cybersecurity compliance for all third-party service providers?
18(b)	PR.DS.S6	1.Does the ASP vendor obtain the source codes for all critical applications from their third-party service providers? 2.Where obtaining the source code is not possible, has the ASP vendor put in place a source code escrow arrangement or other equivalent arrangements to adequately mitigate the risk of default by the third-party service provider? Does the ASP vendor ensure that all product updates and patches/fixes are included in the source code escrow arrangement? 3.For all the software and applications where vulnerabilities will be identified at a later date, does the ASP vendor ensure that the vulnerabilities are mitigated in a time-bound manner? Has the ASP vendor also stipulated timelines in their SLA with their third-party service providers for the timely compliance and closure of identified vulnerabilities? 4.Has the ASP vendor put in place appropriate third-party service providers (including software vendors), risk assessment processes, and controls proportionate to their criticality/risk, **Service Level Agreements (SLAs) and contractual obligations** in order to manage supply chain risks effectively, **Third-party service providers shall be mandated to follow similar or higher standards of information security?** 5.Does the ASP vendor ensure that maintenance and necessary support for applications/software are provided by the third-party service providers (including software vendors) and that this is enforced through a formal agreement?
19	**SEBI and Exchange/Depositories Compliances, Advisory for Financial Sector Organizations**	

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
19(a)	GV.OC.S2	Does the ASP vendor understand, manage, and comply with relevant cybersecurity and data security/protection requirements mentioned in government guidelines/policies/laws/circulars/regulations, etc., issued by SEBI/GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/circular/regulation as and when issued?
19(a)(i)	GV.OC.S2	Do the policy and procedures of the ASP vendor mention and support the following? SEBI/Any other government agency shall at any time perform search and seizure of the ASP vendor's IT resources storing/processing data and other relevant IT resources (including but not limited to logs, user details, etc.) pertaining to the ASP vendor. In this process, SEBI or SEBI-authorized personnel/agencies may access ASP vendor IT infrastructure, applications, data, documents, including other necessary information given to, stored, or processed by third-party service providers?
19(a)(ii)	GV.OC.S2	Do the policy and procedures of the ASP mention and support the following? SEBI/Any other government agency shall at any time perform search and seizure of the ASP's IT resources storing/processing data and other relevant IT resources (including but not limited to logs, user details, etc.) pertaining to the ASP. In this process, SEBI or SEBI-authorized personnel/agencies may access ASP IT infrastructure, applications, data, documents, including other necessary information given to, stored, or processed by third-party service providers?
19(b)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the ASP vendor's policy and procedures includes below clause? All information/ data (classified as Regulatory Data and IT and Cybersecurity Data) that is consumed/ handled by ASP vendors shall be made accessible to SEBI when required. If there is any dependency on external party, ASP vendors shall facilitate information sharing with SEBI by including it in their agreement with external party.
19(c)	PR.AA.S8	Is a strong log retention policy implemented as per government guidelines/policies/laws/circulars/regulations, etc., issued by SEBI/GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023, and as required by CERT-In, NCIIPC or any other government agency?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
19(d)	PR.DS.S1, PR.DS.S2, PR.DS.S3	Does the ASP vendor keep the Regulatory Data available and easily accessible in legible and usable form within the legal boundaries of India? For investors whose country of incorporation is outside India, does the ASP vendor keep the original data available and easily accessible in legible and usable form within the legal boundaries of India? Further, if the Regulatory Data retained within India is not in readable form, does the ASP vendor maintain an application/system to read/analyze the retained data?
19(d)(i)	PR.DS.S1, PR.DS.S2, PR.DS.S3	For SaaS-based cybersecurity solutions and SOC offerings utilized by the ASP vendor where the data is not processed/stored within the legal boundaries of India, is such data classified, assessed, and periodically reviewed (at least once in a year) by the respective IT Committee for ASP vendors or the equivalent body of the ASP vendor? 1.Is such IT and cybersecurity data approved by the Board/Partners/Proprietor annually? 2.Is such data made available to SEBI/CERT-In/any other government agency whenever required within a reasonable time not exceeding 48 hours from the time of request?
19(d)(ii)	PR.DS.S1, PR.DS.S2, PR.DS.S3	During data classification, does the ASP vendor adhere to data security standards and guidelines and other government guidelines/policies/laws/circulars/regulations, etc., issued by SEBI/GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/circular/regulation as and when issued?
19(d)(iii)	PR.DS.S1, PR.DS.S2, PR.DS.S3	For capacity planning and monitoring, does the ASP vendor comply with circulars/guidelines on capacity planning issued by SEBI (and updated from time to time)?
20	**Cyber Security Advisory - Standard Operating Procedure (SOP)**	
20(a)	RS.MA.S1	Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether ASP vendor has complied?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
20(a)(i)	RS.MA.S1	Does ASP have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place? Is the policy approved by Board of the ASP , Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and be reviewed annually by the "Internal Technology Committee" as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy?
20(a)(ii)	RS.MA.S1	Does ASP examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document? Does the Cyber Security incident handling process document define decision on Action/ Response for the Cyber Security incident based on severity?
20(b)	RS.CO.S1, RS.CO.S2, RS.CO.S3	Have ASP vendor reported the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In) and the Exchange (to be reported to the distribution lists: DL-SYSCYB@nse.co.in and DL-INSP@nse.co.in)?
20(c)	ID.RA.S3	ASP should implement the advisories issued by exchanges or any other government agency in their IT environment within a defined timeframe?
21	**Security of Cloud Services:**	
21(a)	21(a)	Does the ASP vendor check the public accessibility of all cloud instances in use to ensure that no server or bucket is inadvertently leaking data due to inappropriate configurations?
21(b)	21(b)	Are the tokens exposed publicly in website source code, any configuration files etc.?
21(c)	21(c)	Has the ASP vendor implemented appropriate security measures for testing, staging, and backup environments hosted on the cloud? Has the ASP vendor ensured that the production environment is properly segregated from these environments? Additionally, has the ASP vendor disabled or removed older or testing environments if their usage is no longer required?
21(d)	21(d)	Has the ASP vendor considered employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
21(e)	21 (e)	Ensure alignment with Governance, Risk, and Compliance (GRC) standards within cloud computing operations and practices. Refer principle 1 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(f)	21(f)	Ensure compliance with established guidelines and protocols in the selection and engagement of cloud service providers. Refer principle 2 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(g)	21(g)	Ensure compliance with data ownership and localization requirements as mandated by relevant regulations and policies within cloud operations. Refer principle 3 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(h)	21(h)	Ensure that the ASP vendor assumes responsibility for maintaining compliance with all relevant cloud computing regulations and standards. Refer principle 4 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(i)	21(i)	Ensure that the ASP vendor conducts thorough due diligence when assessing cloud service providers and their compliance with regulatory requirements. Refer principle 5 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(j)	21(j)	Is robust security controls implemented and maintained to safeguard data and systems in compliance with cloud computing regulations and standards. Refer principle 6 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023?
21(k)	21(k)	Ensure that contractual agreements with cloud service providers align with regulatory obligations to maintain compliance within cloud operations. Refer principle 7 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(l)	21(l)	Are Business Continuity Planning (BCP), Disaster Recovery, and Cyber Resilience measures integrated into cloud operations to ensure compliance with regulatory requirements. Refer principle 8 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023?
21(m)	21(m)	Are strategies implemented to manage vendor lock-in and concentration risks effectively in cloud operations to maintain compliance with regulatory standards. Refer principle 9 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023?

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
21(n)	PR.IP.S15	Software services in the form of SaaS/hosted services used by ASP vendor: 1.Does the ASP vendor submit compliance with the technical specifications mentioned in the hosted services definition for the SaaS/hosted services used by them? 2.Does the ASP vendor also submit compliance with the adoption of hosted services and SaaS as per the various functions of CSCRF, including Governance, Identify, Protect, Detect, Respond, and Recover?
22	**Concentration Risk on Outsourced Agencies:**	
22(a)	GV.SC.S7	Whether the ASP vendor has taken into account concentration risk (where single third-party vendors provide services to multiple ASP vendors) while outsourcing multiple critical services to the same vendor?
22(a)(i)	GV.SC.S7	Whether the organization has identified third-party service providers posing a concentration risk and prescribe specific cybersecurity controls, including audits of their systems and protocols by independent auditors, to mitigate such risks, and does the organization validate that these third-party service providers are meeting their goals of operational resiliency?
23	**Certification of off-the-shelf products**	
23(a)	PR.IP.S15	Customized COTS: Does the ASP vendor ensure that compliance with the tests/audits stated below is met by CERT-In empanelled IS auditing organizations for any customized COTS? a Application security testing: i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc. b. Functional audit c. VAPT after every major release of the application/software

Audit TOR Clause	Standards prescribed by SEBI CSCRF	TOR Details
		d. All critical systems logs integrated with the ASP vendor's SOC by CERT-In empanelled IS auditing organizations for any customized COTS
23(a)(i)	PR.IP.S15	Inhouse developed software: Does the ASP vendor ensure that compliance with the below points is submitted by CERT-In empanelled IS auditing organizations? 1. All the categories of software solutions/applications/products for critical systems used by ASP vendors shall mandatorily pass-through the following tests/audits and compliances: a. Application security testing: i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities. ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc. b. Functional audit c. VAPT after every major release of the application/software d. All critical systems logs shall be integrated with ASP vendor's SOC. e. Audit of firewall configuration, WAF configuration, token configuration and channel identification shall be done. f. Software Bill of Material (SBOM) g. Requirement Traceability Matrix