

TERMS OF REFERENCE (TOR) FOR SYSTEM AUDIT

Sr. No.	Particulars
1	SYSTEM DETAILS:
A	Are periodic reconciliation audits conducted for all the hardware and software assets to confirm compliance to licensing requirements and upgrades?
B	Whether the vendor has provided Provisions for system redundancy, fault tolerance and load balancing?
C	Whether the vendor has provided database redundancy and standby databases (hot standby / cold standby)?
D	Whether the vendor has provided Provisions to monitor system capacity and scalability of system on capacity utilisation?
E	Whether the vendor has provided Provisions for back-up systems and data storage?
F	Whether the vendor has provided Contingency planning in case of technical failure and capacity planning (including periodic evaluation of capacity based on historical and anticipated volumes) should be documented and be available for inspection?
G	Whether the vendor has provided details of feature are in place to ensure that trading member data is maintained confidentially without any third-party access and that the data is maintained separately and independently for each trading member availing the Services?
H	Whether the 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)?
I	Whether the vendor has provided its clients with facilities for 24 X 7 call center / Help Desk?
2	SECURITY REQUIREMENTS:
A	Whether the vendor provides detailed write-up for each of the following areas as per Annexure 1 of circular NSE/MSD/37707? Whether Physical access to the critical systems is restricted to minimum and only to authorized officials.
B	Whether Physical access of outsourced staff/visitors is properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied by authorized employees. i) Whether Access control of staff to system is monitored? ii) Whether Audit trail of all access by staff is maintained? Whether Reconfirmation by second user for critical functions is implemented (second password)?
C	Whether Use of authentication technology i.e.: user ID and First Level password (private code) and Second Level password is implemented?

		<p>i) Whether Automatic expiry of passwords after 60 days and reinitialization of access on entering fresh passwords is implemented</p> <p>ii) Whether Encryption of passwords implemented?</p> <p>D i) Whether Security, reliability and confidentiality of data related to members and clients is maintained?</p> <p>ii) Whether Provisions to ensure that a member / client can see data only pertaining to himself and not other members / clients is maintained?</p> <p>E Whether the vendor ensures that the Records maintained in electronic form should not be susceptible to manipulation?</p> <p>F Whether Logs of all activities / transactions are maintained with proper audit facilities?</p> <p>G Whether Secured Socket Layer (SSL) access through Internet is certified by an approved Certifying Authority?</p> <p>i)Whether appropriate firewall is present between internet and trading setup?</p> <p>ii)Whether the firewall default configuration settings are changed and is appropriately configured to ensure maximum security?</p>
3		SERVICE PROVIDER AGREEMENT (SPA)
	A	Whether the Service Provider Agreement (SPA) between the vendor and desirous trading members is in terms of the model agreement as per Annexure 6 of circular NSE/MSD/37707 and clauses are mutually agreed by member and vendor and are not contradictory to the model agreement.
	B	Whether the vendor has submitted Certified copy to the Exchange?
	C	Whether Service Provider Agreement (SPA) with member is valid at all times?
4		SPA RIGHTS & LIABILITIES OF THE VENDOR
	A	Whether the vendor reserves the rights to restrict entry/movements of the Client or its authorized agents in the premises where the Service is being provided?
	B	Whether the vendor reserve the right to monitor and regulate the mode and manner of the TMs usage of the Service? In runaway/rogue situations, the Service Provider shall be authorized to terminate operations from any of the infrastructure used by the Client, at any time.
5		COMPLIANCE
	A	Whether the vendor is keeping all the information about a client as confidential and separate from the other Clients?

	B	Whether the vendor permits to audit/inspection of whatsoever nature, conducted by the Client or NSEIL or SEBI or any other regulatory authority; In case of audit/inspection by the Client, only such portion of the services as used by the said Client shall be permitted to be accessed by the Client.
	C	Whether the vendor provides operational guidelines to the Client from time to time? as if they were part of this Agreement
	D	Whether the vendor provides Support Services, which shall respond to Client queries or issues and extend support services?
	E	Whether the vendor takes adequate precautions through the use of technology with respect to security aspects as required by the Exchange and/or SEBI and/or any other regulatory?
	F	Whether the vendor provides provisions, in terms of the infrastructure, for the Client to participate in mock / simulated market trading sessions as may be conducted by NSEIL from time to time.
6		RULES AND PROVISIONS
	A	Whether Vendor is permitted to have only one such contract with a particular member at any given point of time for CaaS?
	B	Whether Vendor are liable to all the charges (Annexure 2 of NSE/MSD/37707) as currently applicable to member for availing colocation facility and as updated from time to time. (Auditor to seek conformation from the vendor)
	C	Whether Vendor provides fair, transparent and equitable access to all members availing the service?
	D	Whether Vendor ensures confidentiality of information and data pertaining to each member?
	E	Whether Vendor is responsible for upkeep and maintenance of all infrastructure in his rack/s.
	F	Whether Vendor provides support to the members including BCP provisions, system audit etc. if required by the member.
7	A	Whether the Vendor has informed the members the following? Exchange will provide co-location facility on a best effort basis and Exchange shall not be responsible for any direct/indirect/consequential loss/damage/claim of any kind for any reason whatsoever including but not limited to power failure, air conditioning failure, system failure and loss of connectivity etc. Further, the Exchange shall not be liable for discontinuation of co-location facility owing to legal and/or regulatory requirement. The Exchanges Colocation facility does not have a separate BCP/DR Site and colocation is not available in the exchange's DR facility.
8		ACCESS CONTROL
	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?
	B	Additional Access controls – Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the terminals? Whether additional password requirements are set for critical features of the system?
9		Backup & Recovery (Data, Logs, System Redundancy, Restoration, Alternate Communication etc.)

	A	Backup and Recovery Policy – Whether the Vendor has a well documented policy on periodic backup of data generated from the broking operations?
	B	Log generation and data consistency - Whether backup logs are maintained and backup data is tested for consistency?
	C	System Redundancy – Whether there are appropriate backups in case of failures of any critical system components?
	D	Backup & Restoration- Whether the Vendor has documented policy & procedures for Backup and restoration in order to ensure availability of information? Whether backup logs are verified and tested? Whether backup logs back up logs are maintained? Whether backup media is stored safely in line with the risk involved?
	E	Network / Communication Link Backup- Whether the backup network link adequate in case of failure of the primary link? Whether there is any alternate means of communication including channel for communication for communicating in case of any disruption?
	F	Whether the vendor assures prompt access in the event of failure of any critical system components and they are unable to continue the business in the primary location?
	G	Whether there are suitable backups for failure of any of the critical system components like - Gateway / Database Server Router Network Switch Infrastructure breakdown backup Whether there are suitable arrangements made for the breakdown in any infrastructure components like - Electricity Water Air Conditioning Primary Site Unavailability
	H	Whether vendor has distinct primary and disaster recovery sites (DRS) for technology infrastructure, workspace for people and operational processes? Whether the DRS is 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? Whether any provision for alternate physical location of employees have been made in case of non-availability of the primary site Disaster Recovery? Whether all mission-critical systems been identified and provision for backup for such systems have been made?
10		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)) (Infrastructure Planning, Availability, Governance Policy, Performance Monitoring, Compliance to various organisations policies & procedures, Vulnerability assessment, penetration testing & application security assessments, Information Security policy & Procedure, Information classification & protection etc.)
	A	IT Governance and Policy – whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated? And compliance with these policies is periodically assessed?
	B	IT Infrastructure Planning – whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented? Whether the activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets?
	C	Infrastructure High Availability – <ul style="list-style-type: none"> • Whether the vendor has a documented process for identifying single point of failure? • Whether the vendor ensures that various components pertaining to networks, servers, storage have sufficient redundancy? • Whether the vendor conducts periodic redundancy/contingency testing?

	D	Standards & Guidelines - Whether the vendor maintains standards and guidelines for information security related controls, applicable to various IT functions such as System Administration, Database Administration, Network, Application, and Middleware etc.? Whether the vendor maintains Hardening Standards pertaining to all the technologies deployed within the organization related to Applications, OS, Hardware, Software, Middleware, Database, Network Devices and Desktops? Whether the vendor has a process for deploying OS, Hardware, Software, Middleware, Database, Network Devices and Desktops after ensuring that they are free from vulnerabilities?
	E	Information Security Policy & Procedure - Whether the vendor has documented policy and procedures include the information security policy and if so, are they compliant with legal and regulatory requirements? Is the defined policy. Procedure reviewed on a periodic basis?
	F	Information Security Policy & Procedure - Whether the vendor has any other standards/guidelines like ISO 27001 etc. being followed? Whether the vendor has an Information Security Forum to provide overall direction to information security initiatives based on business objectives?
11		ANTI VIRUS MANAGEMENT
	A	Antivirus Management - Whether the vendor has a documented process/procedure for Antivirus Management? Whether all information assets are protected with anti-virus software and the latest anti-virus signature updates? Whether the vendor periodically scans for virus/malicious code on computing resources, email, internet and other traffic at the Network Gateway/entry points in the IT Infrastructure? Whether the vendor has a documented process/procedure for tracking, reporting and responding to virus related incidents?
	B	Anti-virus - Whether malicious code protection system is implemented? If yes, then Are the definition files up to date? Any instances of infection? Last date of virus check of entire system
	C	Asset Management - Whether vendor has a documented process/framework for managing all the hardware & software assets? Whether vendor maintain a centralized asset repository? Whether periodic reconciliation audits conducted for all the hardware and software assets to confirm compliance to licensing requirements and asset inventory?
	D	Third Party Information Security Management - Whether the vendor has 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? Whether the vendor conducts periodic information security compliance audits/reviews for both onsite and offsite vendors? Are Risks associated with employing third party vendors addressed and mitigated? Whether the defined process/framework periodically reviewed?
12		HUMAN RESOURCE
	A	Human Resources Security, Acceptable Usage & Awareness Trainings - Whether the vendor 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 updated? Whether the vendor performs Background Checks for employees (permanent, temporary) before employment? Whether the vendor conducts Information Security Awareness Program through trainings and Quiz for employees and vendors?

	B	Human Resources Security, Acceptable Usage & Awareness Trainings - Whether the periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors?
13		Patch Management and Vulnerability Assessment and Penetration Testing (VAPT)
	A	Patch management- All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
	B	Vulnerability Assessment and Penetration Testing (VAPT)- Security audit / Vulnerability Assessment and Penetration Testing (VAPT) should be conducted at regular basis and the observation/ gaps of VAPT/Security Audit should be resolved.
14		Measures for Data Protection and Data breach
	A	Data Protection and Data Breach- <ul style="list-style-type: none"> • It is advised to prepare detailed incident response plan. • Enforce effective data protection, backup, and recovery measures. • Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data. • Deploy data leakage prevention (DLP) solutions / processes.