Format of System Audit Report
(To be on the letter head of the System Auditor)

System Audit Report for the period from April 1, 2012 to March 31, 2013

Date:

Annexure A

Areas of Audit		**Auditors Remarks** (Supporting Observations, Findings, References & Substantiation)
1 Organization Policies & Procedures		
Description	**Yes / No**	
Are Policies related to Information Technology & Information Security are available, approved by management and complied		
Is organization structure & roles and responsibilities defined for IT		
Are assets (like application, database, servers, networks etc) identified and ownership assigned towards complete lifecycle of these assets by management.		
Are operators certified for operating the trading systems		
Do incident response procedures exists Are incidents reported, resolved / closed and analyzed for root cause Is escalation of incidents done to management and government organization as applicable, based on criticality, impact and type of incidents		
Do Plans related to business continuity and disaster recovery exist		
Are plans related to business continuity and disaster recovery tested and records related to test available		

2 Perimeter & Environmental Security		
Description	**Yes / No**	
Are equipment and resources (people, systems, database, network and application) are sited in a manner to protect and prevent risks from environmental threats & hazards, and opportunities for unauthorized access.		
Physical Access to the area is controlled by reliable controls and only authorized users have access to these areas and to prevent misuse of facility by unauthorized persons		
Logs of access to these areas maintained and reviewed		
Is storage of backup secured commensurate to the risks involved and backup stored at a geographically separate location from primary		
Contact list for emergency / crisis exists and updated		
3 Access Control		
Representation		
AC_Pro: Access Control Procedure / Process		
AC_Auth: Access Control Authentication		
AC_Pwd: Access Control Password		
Each of the above have specific attributes specified in number.		
Description	**Yes / No**	
AC_Pro1 Is approval and authorization a required process for creating user and providing access (physical, system, database, application)		
AC_Pro2 Are users created by authorized personnel		
AC_Pro3 Is there track of user id's created, disabled, enabled, deleted, unlocked, log of all such events maintained		
AC Pro4 Are passwords (of systems / database / application) changed in event of employee / vendor staff leaving the company / transfers.		

AC Pro5 In case of new user / password resets; is password communicated to user securely		
AC Pro6 A process exists to block / suspend the user (id) on request from user (case of loss of device / malicious activity)		
AC_Auth1 Does the system (Application / System / Database) challenges (prompts) all user for authentication		
AC_Auth2 Is the mechanism for authentication strong enough so as to control the threats that may be applicable		
AC_Auth3 Are users uniquely identifiable with a unique user id		
AC_Auth4 Are there generic ids existing for access		
AC_Auth5 Are two factor authentication for login session implemented for all orders emanating using internet protocol.		
AC_Auth6 Is Public Key Infrastructure (PKI) based implementation using digital signatures deployed for authentication, supported by one of the agencies certified by government of India.		
AC_Auth7 Are the two factors in the two factor authentication framework different		
AC_Pwd1 Does System requires changing of password when the user logs in for the first time.		
AC_Pwd2 Are users automatically disabled (Locked) on entering erroneous password on three consecutive occasions		
AC_Pwd3 Does system disable (block/lock) user automatically on expiry of password.		
AC_Pwd 4 Are controls implemented to ensure that password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical.		
AC_Pwd5 Are controls existing to ensure that the changed password cannot be the same as of the last password		
AC_Pwd6 Are controls existing to ensure that the Login id of the user and password should not be the same.		

AC_Pwd7 Are controls existing to ensure that the Password should be of minimum six characters and not more than twelve characters.		
AC_Pwd8 Are controls existing to ensure that all password are secured by encryption mechanism and that encryption mechanism is adequate enough to provide safety from applicable risks		
AC_PWD9 System ensures that password is masked at time of entry.		
AC_SS Does the system allow only authorized administrative users to terminate a user's session.		
4 IT Systems and System Security		
Description	**Yes / No**	
Are systems adequately managed, controlled and secured		
Do systems provide security to applications, database and data stored (data at rest) adequately using mechanism such as encryption		
File system:		
All volumes of the server hosting the database and / application has file system that offers enhanced security – For Ex: EFS / NTFS for windows, Vxfs- for HP Unix, ext3 for Linux etc.		
Directory / File Sharing:		
Default file &directory shares and simple file sharing if offered by the operating system are disabled.		
Sharing if any is authorized		
Are guest accounts disabled / hashed out / deleted		
Patches, hot fixes and service packs are updated after appropriate testing		

Auditing is enabled for events like Account logon events, Account Management, Object access, Policy change, privilege use, system events		
Do all users adhere to Access Controls like described in (Section 3 of Annexure A)		
AC_Pro: Access Control Procedure / Process		
1 AC_Pro1		
2 AC_Pro2		
3 AC_Pro3		
4 AC_Pro4		
4 AC_Pro5		
5 AC_Pro6		
AC_Auth: Access Control Authentication		
1 AC_Auth1		
2 AC_Auth2		
3 AC_Auth3		
AC_Pwd: Access Control Password		
1 AC_Pwd1		
2 AC_Pwd2		
3 AC_Pwd3		
4 AC_Pwd4		
5 AC_Pwd5		
6 AC_Pwd6		
7 AC_Pwd7		
8 AC_Pwd8		
9 AC_SS		

Are system clocks synchronized to atomic clock to ensure synchronization.		
Are critical systems located behind firewall with default rules to deny all traffic and only identified specific application, database and system protocols are allowed.		
The system is adequately protected from malware (such as viruses, spyware ..etc) with controls such as antimalware / antivirus system and that rules / definitions are updated		
The entire system is scanned periodically to ensure protection.		
5 Network and Network Security		
Description	**Yes / No**	
Are networks adequately managed, controlled and monitored		
Does network provide security to the data, systems and applications in the network.		
The network security protocols and interface standards deployed are as per prevalent industry standards		
Do all users adhere to Access Controls like described in (Section 3 of Annexure A)		
Is information travelling over network (Wired & / wireless) adequately protected with mechanism such as VPN, TLS /SSL / . WPA2.		
Is backup network link available in case of failure of the primary link to the BSE		
Is backup network link available in case of failure of the primary link connecting the customers		
Does alternate communications path between employees and the firm exists		
Does alternate communications path with critical business constituents, banks and regulators exists		

□ Verify location(s) of nodes in the network		
□ Verify number of nodes in diagram with actual		
□ Date of submission to BSE.		
Are parameters identified and logged to enable traceability and non-repudiation of orders / actions performed with relevant details like IP address, MAC address, time and other data		
Are network device clocks synchronized to atomic clock		
Are network segments used to segregate critical, non critical and user systems		
Are network devices appropriately patched / upgraded with latest firmware		
Log events are identified, monitored, reviewed and escalated		
6 Database and Database Security		
Description	**Yes / No**	
Do all users adhere to Access Controls like described in (Section 3 of Annexure A)		
AC_Pro: Access Control Procedure / Process		
1 AC_Pro1		
2 AC_Pro2		
3 AC_Pro3		
4 AC_Pro4		
4 AC_Pro5		
5 AC_Pro6		
AC_Auth: Access Control Authentication		
1 AC_Auth1		
2 AC_Auth2		

3 AC_Auth3		
AC_Pwd: Access Control Password		
1 AC_Pwd1		
2 AC_Pwd2		
3 AC_Pwd3		
4 AC_Pwd4		
5 AC_Pwd5		
6 AC_Pwd6		
7 AC_Pwd7		
8 AC_Pwd8		
9 AC_SS		
Database – Firewall		
DB FW1 - Is the database server located behind a firewall with default rules to deny all traffic.		
DB FW2 - Is the database server firewall is opened only to specific application or web servers, and firewall rules do not allow direct client access.		
DB FW3 - Firewall rule change control procedures are in place and notification of rule changes are distributed to System Administrators (SAs) and Database Administrators (DBAs).		
DB FW4 - Are firewall rules for database servers maintained and reviewed on a regular basis by SAs and DBAs.		
Secured Environment		
DB_SE1 - Is the database software installed by exclusive user. Is this user, super user / Administrator		
DB_SE2 -Is the database software owner account granted the minimum set of operating system rights necessary for database operation.		

DB_SE3 -IS the database software version is currently supported by the vendor or open source project.		
DB_SE4 -Are all unused or unnecessary services or functions of the database are removed or turned off.		
DB_SE5 -Are unneeded default accounts are removed, or else passwords are changed from defaults.		
DB_SE6 -Are Null passwords used, and have the temporary files from the install process that may contain passwords are removed.		
DB_SE7 -Database software is patched to include all current security patches. Provisions are made to maintain security patch levels in a timely fashion.		
DB_SE 8 Are all old setup files / test databases / sample databases deleted / secured / access removed		
DB_SE 9 log events are identified audit trails enabled, reviewed and monitored		
DB SE 10 the clock of the system hosting the database is synchronized with atomic clock		
Database – IML		
DB_IML1- Do all users of system adhere to Access Controls like described in Section 4 Annexure A		
DB_IML2- The IML database is hosted on a secure platform and adheres controls like mentioned in Section 4 Annexure A..		
DB_IML3- The information in the database used to store/ retrieve transaction information is secured with controls		
Are system clocks of system hosting the database synchronized to atomic clock.		
7 Encryption		
Description	**Yes / No**	
Is all data transmission between the client & broker / member secured through end to end encryption through a secure		

standardized protocol*		
Does the key size used for encryption adhere to the policies & / guidelines mandated by relevant authorities*		
Key management procedures for decrypting are documented, available to more than one (authorized) person's, approved by the data proprietor and procedures for secure key management followed.		
Are the encryption keys stored in secure location and access procedures documented.		
SSL / TLS used by web based application		
Are certificates issued to the member / broker organization		
Are the certificates used on the server facilitating confidential information – like trade data		
Is the login page and all subsequent authenticated pages exclusively accessed over TLS/SSL		
Provide the following details		
Certificate Issuer: (Name)		
Validity Not Before: (Date)		
Validity Not After: (Date)		
In case of Client Server application model (Thick Client)		
Does the application architecture adequately ensure security of information sent over internal / external network		
Is the information transmitted in encrypted form		
Please provide supporting letter from vendor on his letterhead.		
Do the encryption deployed and procedures related to it align to policies and regulations of DoT (Department of Telecom) & / Information Technology Act 2000		

8 Audit Log & Monitoring		
Description	**Yes / No**	
ALM1 - Are audit logs for systems, databases, networks and applications appropriately identified and enabled for recording of relevant actions and events.		
ALM2 - All session initiation and termination events are logged and audited.		
ALM3 - Are logs reviewed and exceptions / findings if any escalated.		
ALM4 - Are systems adequately capable of noting all transactions conducted with sound audit trails available for all transactions		
9 Capacity Management		
Description	**Yes / No**	
CM1 - Are the resources monitored, tuned and calculations made for future capacity requirements to ensure the required performance.		
CM2 - Are data storage, backup systems, system capacities adequately available for handling data transfer, and arranged for alternative means of communications in case of Internet link failure.		
CM3 - Do systems have built-in high system availability to address any single point of failure		
CM4 - Are backup resources available to ensure that all essential information and software can be backed up and tested for restoration		
10 Pre-Trade Risk Control: Value Limit per Order etc.		
Are the following SEBI and BSE Limited circulars complied to 1 - SEBI circular CIR/MRD/DP/34/2012 dated December 13, 2012		
2 – BSE Limited circular no. 20121214-14 dated December 14, 2012		
3 - BSE Limited circular no. 20130108-20 dated 08 Jan 2013		

11 Online Risk Management Tools & Order Entry		
Description:	**Yes / No**	
Whether Exchange circular 20121101-16 dated November 1, 2012 has been complied with ? The Risk Management Tool has provisions for setting parameters such as		
Trading Limits		
Exposure Limits		
Order Quantity Limits		
Order Value Limits		
Price range checks		
Net Position Limits		
The risk management tool ensures the following for all orders, before being placed		
Online risk assessment of the orders to be placed.		
Online risk monitoring of the orders being placed.		
Online risk management of the orders being placed.		
Does system allow only authorized administrative user to alter the risk parameters of users		
Does system allow manual placement (through approved mechanism) for allowing orders that do not fit the system based risk control parameter.		
Are orders successful / unsuccessful or valid / invalid are logged, reviewed and auditedby the risk management system		
Appropriate validation of all risk parameters is done before placing the order		

Order Entry		
Description	Yes / No	
Only duly authorized client's orders are allowed to be placed.		
Order entry for Pro types of orders is executed through specific user ids.		
The system does not have an order matching system and all orders are passed on to the exchange trading system for matching. on the basis of priority of receipt of the orders from the clients		
12 Features of System		
Scope: Application		
Description	**Yes / No**	
Are all servers used for routing orders to BSE Ltd trading system are hosted (geographically located) in India.		
Does system allows only authorized and validated users to establish a session with the system.		
Does system allow only authorized administrative users to terminate a users session.		
System deployed routes the orders in neutral manner		
Features of system have been submitted to BSE Ltd.		
Does system have unique identification numbering system for all orders to identify trades uniquely and all orders with time stamp are available with reference to the unique identification number		
In case no activity by the client, does the system provide automatic trading session logout		
In case of failure of service / system / facility (for ex - network, application) , alternative modes of communications for placing orders are available		
Price Broadcast		

Does system allows order entry and confirmation of order is provided to the user on submission of the order.		
Does system provide order modification / cancellation facilities.		
Does system have capability to provide trade confirmation to the user, along with history of trades for the day.		
Allow for checking the pending orders i.e. the orders that have not yet traded or partially traded.		
Provides feature of reporting the trades happened		
Allows for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations.		
Whether the System uses authentication measures like smart cards, biometric authentication etc.		
Whether the system has a second level of password control for critical features		
Is periodic verification of UCC & location details of data done		
Wherever applicable session login credential details are not stored on the devices used for trading		
Are features available in the system to identify IML-IBT/ STWT (Mobile) / SOR / DMA orders, trades and related data.		
Reporting		
R1: Are there features / facilities available to generate MIS reports for reporting to exchange, SEBI or other relevant regulators.		
R2: Are procedures / processes set for reporting and lists / checklist used for such purposes.		
13 IML –IBT (Internet Based Trading) (Order Routing System)		
Scope: Application, Database, System & Network as applicable		
Description	**Yes / No**	

Organizational policies & procedures exists and are followed for IML / IBT (Ref Section 1 of Annexure A)		
Perimeter & Environmental Security controls exists and are followed (Ref Section 2 of Annexure A)		
Controls related to access exists (Ref Section 3 of Annexure A)		
IT Systems and System Security Controls exists and are adhered to (Ref Section 4 of Annexure A)		
Network and Network Security controls exists and are adhered to (Ref Section 5 of Annexure A)		
Database deployed adhere to database and database security controls (Ref Section 6 of Annexure A)		
Encryption controls are deployed and applicable procedures are adhered to (Ref Section 7 of Annexure A)		
Audit logs for activities are registered and monitoring controls exist (Ref Section 8 of Annexure A)		
Capacity related procedures, processes and controls are deployed and monitored (Ref Section 9 of Annexure A)		
Online Risk Management Tools and Order Entry controls as applicable are followed for all orders placed (Ref Section 10 of Annexure A)		
Are features of system adequately available, controlled as applicable (Ref Section 11 of Annexure A)		
Provide Installation Details (IML) Total number of IML IDs IML version /IML Trading Software Version Risk Administration / Manager Version Front End / Order Placement Version Number of Users Logged In / hooked on to the network incl. privileges of each Number of authorized users on the system Number of active clients Activity & System Logs		

Are processes & procedures implemented to ensure that norms mentioned in SEBI Circular / Directives regarding to Internet Based Trading adhered to (refer 1 - SMDRP/POLICY/CIR-06 /2000 Dated January 31, 2000 2 - CIR/MRD/DP/8/2011 Dated June 30, 2011) Are they complied		
With reference to BSE Limited notice – notice no - 20130128-2; dated 28 Jan 2013 With the implementation of Two-factor authentication, is the automatic expiry of password revised .		
14 Securities Trading Using Wireless Technology [Mobile Trading]		
Scope: Application, Database, System & Network as applicable		
Description	**Yes / No**	
Are all relevant requirements as applicable to internet based trading being adhered to securities trading using wireless technology		
Is STWT order routing is available to all clients and they are communicated all features, possible risks, rights, responsibilities and liabilities associated with the STWT facility.		
Does the client desirous of availing such (STWT) facility has to do so by entering into a broker-client agreement, as applicable. For the existing clients, is the same implemented through an addendum to the existing broker-client agreement, as applicable.		
In case of issues due to form factor, has it been ensured that minimum information has been given with addresses of the internet web site /web page where detailed information would be available.		
The application used for mobile trading is		
1 – 3rd party solution from empanelled vendor with BSE		

2 – in house developed mobile trading solution approved by BSE.		
Please provide references for the above applicable cases.		
Is mobile trading an extension of internet based trading (Thin Client)		
In case it is a thick client provide the details of the architecture		
Order Status information is adequately informed to the user through appropriate mechanism		
Appropriate validation of all risk parameters before placing the order is done prior to placing order in Mobile Trading		
Organizational policies & procedures exists and are followed for STWT (Ref Section 1 of Annexure A)		
Perimeter & Environmental Security controls exists and are followed (Ref Section 2 of Annexure A)		
Controls related to access exists (Ref Section 3 of Annexure A)		
IT Systems and System Security Controls exists and are adhered to (Ref Section 4 of Annexure A)		
Network and Network Security controls exists and are adhered to (Ref Section 5 of Annexure A)		
Database deployed adhere to database and database security controls (Ref Section 6 of Annexure A)		
Encryption controls are deployed and applicable procedures are adhered to (Ref Section 7 of Annexure A)		
Audit logs for activities are registered and monitoring controls exist (Ref Section 8 of Annexure A)		
Capacity related procedures, processes and controls are deployed and monitored (Ref Section 9 of Annexure A)		
Online Risk Management Tools and Order Entry controls as applicable are followed (Ref Section 10 of Annexure A)		

Are features of system adequately available, controlled as applicable (Ref Section 11 of Annexure A)		
Are processes & procedures implemented to ensure that norms mentioned in SEBI Circular / Directives regarding to STWT adhered to (refer - 1 - CIR/MRD/DP/25/2010 Dated August 27,2010 2 - CIR/MRD/DP/8/2011 Dated June 30, 2011) Are they complied		
With reference to BSE Limited notice – notice no - 20130128-2; dated 28 Jan 2013 With the implementation of Two-factor authentication, is the automatic expiry of password revised.		
15 Smart Order Routing (SOR)		
Scope: Application, Database, System		
Description	**Details**	
Is smart order routing is available to all clients and they are communicated all features, possible risks, rights, responsibilities and liabilities associated with the smart order routing facility.		
Does the client desirous of availing such (SOR) facility has to do so by entering into a broker-client agreement, as applicable. For the existing clients, is the same implemented through an addendum to the existing broker-client agreement, as applicable.		
Are all type of trades / orders executable as chosen by the user and user requests for specific orders not to be used under SOR facility recorded and documented		
Is SOR permitted for all orders without restricting any specific type of order, and that choice of orders is left to client.		

Organizational policies & procedures exists and are followed for SOR (Ref Section 1 of Annexure A)		
Perimeter & Environmental Security controls exists and are followed (Ref Section 2 of Annexure A)		
Controls related to access exists (Ref Section 3 of Annexure A)		
IT Systems and System Security Controls exists and are adhered to (Ref Section 4 of Annexure A)		
Network and Network Security controls exists and are adhered to (Ref Section 5 of Annexure A)		
Database deployed adhere to database and database security controls (Ref Section 6 of Annexure A)		
Encryption controls are deployed and applicable procedures are adhered to (Ref Section 7 of Annexure A)		
Audit logs for activities are registered and monitoring controls exist (Ref Section 8 of Annexure A)		
Capacity related procedures, processes and controls are deployed and monitored (Ref Section 9 of Annexure A)		
Online Risk Management Tools and Order Entry controls as applicable are followed for all orders placed (Ref Section 10 of Annexure A)		
Are features of system adequately available, controlled as applicable (Ref Section 11 of Annexure A)		
Order Decision		
OD1: Are all activities related to orders and trade logged to facilitate audit trail and records maintained along with the details such as orders, trades and data points for the basis of decision		
OD2: is there facility for logging data related to orders / trades (on random sampling / continuous basis) used to support the decision of trade / order. Is it being used, reviewed and audited.		

Does the application monitors best bids and offers and updates instantly as the market moves:		
Does the application provide transparency in terms of time delays		
Are controls available and implemented to ensure that orders thorough SOR are placed at recognized stock exchanges only.		
Does functionality exists to specify for individual orders for which they do not want to route the order using SOR		
Are well documented records available to support of not using SOR for particular order by client (who has availed SOR facility)		
Are processes & procedures implemented to ensure that norms mentioned in SEBI Circular / Directives regarding to STWT adhered to (for Ex 1 - CIR/MRD/DP/26/2010 Dated August 27, 2010 2 - CIR/MRD/DP/36/2010 Dated December 09, 2010) Are they complied		
16 Direct Market Access		
Scope: Application, Database, System		
Description	**Yes / No**	
Clients having access to DMA have been provided access after execution of agreement with conditions as prescribed in the "Model Agreement" by BSE and such agreement is valid currently.		
Organizational policies & procedures exists and are followed for SOR (Ref Section 1 of Annexure A)		
Perimeter & Environmental Security controls exists and are followed (Ref Section 2 of Annexure A)		
Controls related to access exists (Ref Section 3 of Annexure A)		
IT Systems and System Security Controls exists and are		

adhered to (Ref Section 4 of Annexure A)		
Network and Network Security controls exists and are adhered to (Ref Section 5 of Annexure A)		
Database deployed adhere to database and database security controls (Ref Section 6 of Annexure A)		
Encryption controls are deployed and applicable procedures are adhered to (Ref Section 7 of Annexure A)		
Audit logs for activities are registered and monitoring controls exist (Ref Section 8 of Annexure A)		
Capacity related procedures, processes and controls are deployed and monitored (Ref Section 9 of Annexure A)		
Online Risk Management Tools and Order Entry controls as applicable are followed for all orders placed (Ref Section 10 of Annexure A)		
Are features of system adequately available, controlled as applicable (Ref Section 11 of Annexure A)		
Are unique identification numbers given as in case of internet based trading, to identify trades and orders done using DMA and log of events with timestamp are available with reference to the unique identification number and such records are available for minimum of 5 years		
Are there controls available and implemented in the system for DMA order masking to prevent front running of the orders.		
Appropriate validation of all risk parameters is done to ensure that trading limits/ exposure limits/ position limits are set for all DMA clients		

Details of the IML ID's used by the trading members:

Clearing No: _____

IML ID	Software Details(Inhouse/ Vendor Name)	Purpose of procurement	IML Location (Address)	Date of activation.

1.	Whether the required details of all the Ids created in the IML server of the trading member, for any purpose (viz. administration, branch administration, surveillance, risk management, trading, testing, etc) and any changes therein, have been uploaded to the Exchange? If no, please give details	YES/NO
2.	Whether all the IML user ids created in the IML server of the trading member has been mapped to 16 digits LOCATION ID on one-to-one basis and a record of the same is maintained?	YES/NO

Annexure B (Optional)

Areas of Audit		Auditors Remarks (Supporting Observations, Findings, References & Substantiation)
17 Policies, Procedures and Documents Availability		
Description	**Yes / No**	
Information Security Policy		
Password Policy		
User Management and Access Control Policy		
Network Security Policy		
Application Software Policy		
Backup Policy		
Change Management Policy		
BCP and Response Management Policy		
Audit Trail Policy		
Other policies followed if any and its reference		

18 Approvals, undertaking, agreements, policies:	
Description	**Yes / No**
1 - Internet Trading 2 - SOR 3 - Wireless (Mobile Trading) 4 - DMA For the above segments are the following documents available Copy of application to exchange Approval / Copy of approval from exchange Undertaking(s) provided as per relevant circulars as required by exchange / SEBI	
Undertaking provided regarding the IML system as per relevant circulars	
Whether the Insurance policy of the Member covers the additional risk of usage of IML and or Internet Trading	

19 Change Management	
Description	**Yes / No**
Changes to the system supporting trading are made in a planned manner	
Changes are made by duly authorized personnel	
Risk involved in the implementation of the changes duly factored in	
The implemented change duly approved and process documented	
The change request process documented	
Change implementation process supervised to ensure system integrity and continuity	
User acceptance of the change documented	
Unplanned changes duly authorized and the manner of change documented later	
SDLC documentation and procedures if the installed IML system is developed in-house	

20 User Management	
Description	**Yes / No**
No. of user Ids created	
All users are uniquely identified through issue of unique IML ids.	
No. of Users are deleted and logs are maintained	
No. of Users are disabled and logs are maintained	
No. of users reissued and logs are maintained	
No. of users whose accounts are locked with logs	
The users in the system are created by authorized personnel at server level	

21 Redundancy & Backup in case of System Failure		
Description	**Yes / No**	
Backups for the critical system components		
Gateway / Database Server		
Audit Trails		
IML router		
Network Switch		
Communication lines		
Infrastructure breakdown backup		
Electricity		
Water		
Air Conditioning		
Alternate physical location of employees been made in case of non availability of the primary site		
Provisions for Books and records backup and recovery (hard copy and electronic).		
Mission-critical systems been identified and provision for backup for such systems been made		
Are backup and recovery procedures defined, approved and documented		
Are backup and restoration records and logs maintained.		
Are backup media stored safely in line with risks		

22 Daily Operational Activities	
Description	**Yes / No**
Provision for Begin of day activity	
Audit Trails	
Access Logs	
Transaction Logs	
Backup Logs	
Alert Logs	
Activity Logs	
Misc (Please specify):	
Provision for End of day activity	
System for log monitoring, escalation & corrective measures taken, if any.	
The IML solution should not in any manner suggest to the user by default the name of Exchange, scrip and segment etc. It is the user who should have the option to select the same.	

23 Response Procedures		
Description		
Access Control failure		
Beginning of Day failure		
End of Day failure		
Other system Processes failure		
24.Other information		
Description		
Gateway Parameters □ Trader ID		
Cash Segment □ IML ID □ IP Address □ (BSE Network) □ VSAT ID □ Leased Line ID		
F&O Segment □ DIML ID □ IP Address □ (BSE Network) □ VSAT ID □ Leased Line ID		
25. Auditor comments towards data and information related to trade and orders		
Confidentiality:		
Integrity:		
Availability:		
Non-Repudiation:		

Annexure C (Mandatory)

INFORMATION SYSTEM AUDIT OF_____

Sr No	Area of Audit	Classification of Controls in Annexure A S / A / I	Classification of Controls in Annexure B S / A / I
1	Organization structure exists and supports governance through policies, procedures, proceses and guidelines.		NA
2	Systems & processes related to perimeter and environmental security controls exists		NA
3	Access, Authentication and Authorization to systems (systems, database, os, networks etc) is commiserate with the importance of the systems		NA
4	Systems follow policies & procedures to protect from threats that might exploit the system.		NA
5	Network & Network Security follow policies & procedures to protect from threats that might exploit the system.		NA
6	Database systems follow policies & procedures to protect from threats that might exploit the system.		NA
7	Processes and procedures for encryption deployed for protection of data is established		NA
8	Audit logging and monitoring are established to identify and determine accountability of actions performed.		NA
9	Processes and procedures followed for capacity management are established.		NA
10	Pre-Trade risk control: Value limit per order etc. are implemented and adhere to all applicable circulars from SEBI & BSE Limited		NA
11	Online risk management tool and order entry are supported.		NA
12	Features of system are established and implemented		NA
13	IML / IBT systems are controlled and adhere to all applicable circulars from SEBI & BSE Limited		NA

14	Securities Trading using Wireless Technology (Mobile Trading) systems are controlled and adhere to all applicable circulars from SEBI & BSE Limited		NA
15	Smart Order Routing systems are controlled and adhere to all applicable circulars from SEBI & BSE Limited		NA
16	Direct Market Access systems are controlled and adhere to all applicable circulars from SEBI & BSE Limited		NA
17	Are policies available, implemented and reviewed for implementation.	NA	
18	Are communication documents viz application, approval, & undertaking available, valid and secured.	NA	
19	Is change management an established process and procedures for change are implemented in controlled manner.	NA	
20	Is user management done according to policy defined and procedures adhere to the policy, records for implementation and adherence are available.	NA	
21	Is redundancy and backup available and tested in case of system failure.	NA	
22	Are daily operational activities controlled and logged to demonstrate control	NA	
23	Are response procedures available and records of use indicate established procedure.	NA	
24	Is information related to parameters available and updated periodically	NA	
25	Any other comment by auditor towards data and information related to trade and orders	NA	

Declaration:
Member Summary

Sr #	Trading Facilities	Trading Facility Offered? (Yes / No)	Trading Facility Audited? (Yes / No)
1	IML – IBT Trading (Internet Based Trading)		
2	STWT (Securities Trading Using Wireless Technology)		
3	SOR (Smart Order Routing)		
4	DMA (Direct Market Access)		

All the branches where IML-IBT / STWT/ DMA facility is provided, have been audited and consolidated report has been submitted.

I undersigned assure of circulars issued by SEBI an BSE Limited have been referenced for checking the compliances and that the contents of the report as per audit performed by me and declare there is no conflict of interest with respect to the member being audited.

Audit recommendations (if any) in relation to System Audit report for the year ended March 31, 2012 that have been duly implemented / not implemented are mentioned separately as annexure (as a part of System Audit report).

In case you have been rated as "Medium/Weak" in any areas by System auditor between April 1, 2012 to March 31, 2013 (prior to granting approval for Internet based Trading/ Direct Market Access/ SOR/ Wireless securities trading except for Algorithmic Trading) please submit "Action Taken Report" duly certified by your system auditor detailing the actions taken by you on various individual "Medium/ Weak areas.

_____

Signature

(Full Name of the Auditor & Auditing firm)

CISA Registration Number:

Date:

Place:

Note: Criteria for Evaluation of Controls are indicated below, based on these "Area of Audit" as mentioned in Annexure A & B are to be rated.

Evaluation of Controls	Description
Strong	Controls are said to be Strong if objectives are fully complied with and no material weaknesses are found.
Adequate	Controls are said to be Adequate if objectives are substantially complied with and no material weakness result in substantial risk exposure due to non-compliance Compensatory controls exist which reduce the risk exposure to make it immaterial vis –a-vis the non-compliance with the criteria.
Inadequate	Controls are said to be Inadequate if objectives are not complied with. Compensatory controls fail to reduce the risk so as to make it immaterial vis-à-vis the non-compliance with the compliance criteria.