**Annexure A**

**Auditor’s Report**

**Non-Exchange Frontend (ETI Facility) / Algorithmic Trading (AT Facility)**

**(To be on the letterhead of the system auditor, all pages to be duly stamped and signed)**

**BSE Trading Member Code:**

**BSE Trading Member Name:**

**Areas of Audit:**

* Risk Management
* Security Policy and implementation
* Capacity Management
* Disaster Recovery and Backups
* Vulnerability Test

The detailed findings will be grouped under the above broad categories and classified as ‘Strong’, ‘Medium’ or ‘Weak’ and overall audit rating will be given**.**

| **Controls / Processes** | **Test Case** | **Results, Observations & Control Risk** | **Auditor’s Risk** |
| --- | --- | --- | --- |
| **Location Confirmation**  **The installed ETI / AT system features are as prescribed by the BSE.**  **The installed ETI / AT system parameters are as per BSE norms** | Whether order routing server for ETI / AT is located in India  System network and Network Diagram  Risk Management Tools  Should allow for risk management of the orders placed and online risk monitoring of the orders being placed.  ETI / AT Version   * Order Gateway Version * Risk Administration / Manager Version | Results | Opinions |
| **Trading Process**  **The installed ETI / AT system allows for placing of trades only for authorized clients**  **Risk Management**  **The installed ETI / AT system is capable of assessing the risk of the client as soon as the order comes in and informs the client of acceptance/rejection of the order within a reasonable period.**  **Order /Trade Limit Controls**  **The installed ETI / AT system provides a system based control facility on the trading limits of the clients and exposures taken by the clients including set pre-defined limits on the exposure and turnover of each client.**  **Order Reconfirmation Facility**  **The installed ETI / AT system provides for reconfirmation of orders which are larger than that as specified by the member’s risk management system.**  **Execution of Orders / Order Logic**  **The installed ETI / AT system provides a system based control facility over the order input process** | User id Verification  Only duly authorized User’s orders are allowed to be placed.  Order Parameters based on the respective risk profile of the user  There is online risk assessment of all orders placed through the ETI / AT system with following checks :   * Order Value per order should not exceed as specified in RMS (not exceeding the maximum limit as specified by Exchange) * Order Quantity per order should not exceed as specified in RMS * Spread order value and quantity limit per order should not exceed as specified in RMS. * Cumulative value of all unexecuted / open orders should not exceed as specified in RMS at client level * Order value limit at client level * Order value limit at branch level * Security-wise order limits at client level   Only orders that are within the parameters specified by the risk management systems are allowed to be placed.  Are there provisions for setting trading limits, exposure limits, position limits, order quantity limits order value limits, price range checks, Net Position limits for all ETI / AT users based on risk assessment, credit quality and available margins of the client. Also appropriate limits for securities which are subject to FII limits as specified as RBI.  The system has a manual override facility for allowing orders that do not fit the system based risk control parameters  Order Numbering Methodology  If the system is enabled for ETI / AT the system has an internal unique order numbering system  Order Matching  The system does not have any order matching function resulting into cross trades of the clients orders of a trading member with each other. All orders are passed on to the exchange trading system for matching.  Whether Broker is using similar logic/ priorities as used by Exchange to treat ETI / AT user orders.  Whether ETI / AT orders are having unique flag/ tag as specified by the Exchange. | Results | Opinions |
| **Application Access Control**  **The installed ETI / AT system provides a system based access control over the ETI / AT server as well as the risk management and front end dealing applications while providing for security**  **Session Security**  **The installed ETI / AT system provides for session security for all sessions established with the ETI / AT server by the front end application.**  **Database Security**  **The installed ETI / AT system has sufficient controls over the access to and integrity of the database**  **Encryption**  **The installed ETI / AT system uses confidentiality protection measures to ensure session confidentiality.** | Access controls   * The system allows access to only authorized users * The system has appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager * The system has a password mechanism which restricts access to authenticate users.   Session Security   * The system uses session identification and authentication measures to restrict sessions to authorized user only. * The system uses session security measures like encryption to ensure confidentiality of sessions initiated.   Database Security   * The access to the ETI / AT database is allowed only to authorized users / applications. * The ETI / AT database is hosted on a secure platform. * The ETI / AT database stores all the details of user ids activated for ETI / AT along with user names and passwords securely. * Frequency of antivirus patch updation   Session Encryption   * The system uses session confidentiality protection mechanisms * The system uses a secure storage mechanism for storing of usernames and passwords. * The system adequately protects the confidentiality of the users’ trade data. | Results | Opinions |
| **The installed ETI / AT 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 ETI / AT system has a provision for off line monitoring and risk management as per the requirements of BSE and includes reports / logs on   * Number of Authorized Users * Activity logs * Systems logs * Number of active clients * Review of logs (activity/system/alert/incident) |  |  |
| **The installed ETI / AT system Authentication mechanism is as per the guidelines of the BSE** | The installed ETI / AT system’s uses passwords for authentication.  The password policy / standard are documented.  The system requests for identification and new password before login into the system.  The installed ETI / AT system’s Password features include   * The Password is masked at the time of entry. * System mandated changing of password when the user logs in for the first time. * Automatic disablement of the user on entering erroneous password on three consecutive occasions. * Automatic expiry of password on expiry of reasonable period of time as determined by member. * 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 password * 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 reasonable minimum length (and no arbitrary maximum length cap or character class). * System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time. * System control ensures Re-initialisation of access on entering fresh passwords. | Results | Opinions |
| **The Installed ETI / AT systems backup capability is adequate as per the requirements of the BSE for overcoming loss of product integrity.** | Are backups of the following system generated files maintained as per the BSE guidelines?   * At the ETI / AT server/gateway level * Database * Audit Trails * Reports   At the ETI / AT user level   * Market Watch * Logs * History * Reports * Audit Trails * Alert logs   Are backup procedures documented?  Are backup logs maintained?  Have 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? | Results | Opinions |
| **The installed ETI / AT system parameters are as per BSE norms** | Gateway Parameters   * Trader ID   Market Segment   * IP Address * (BSE Network) * VSAT ID * Leased Line ID |  |  |
| **Trades Information**  **The installed ETI / AT system provides a system based control facility over the trade confirmation process**      **Settlement of Trades**  **The installed ETI / AT system provides a system based reports on contracts, margin requirements, payment and delivery obligations** | Trade Confirmation and Reporting Feature  Should allow confirmation and reporting of the orders that have resulted in trade        Margin Reports feature  Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | Results | Opinions |
| **To ensure information security for the Organization in general and the installed ETI / AT system in particular policy and procedures as per the BSE requirements must be established, implemented and maintained.** | Systems & procedures:  Whether installed systems & procedures are adequate to handle ETI / AT orders/ trades?  Maintenance of User details:  Whether details of users activated for ETI / AT facilities is maintained along with user name, unique identification of user, authorization levels.  Does the organization’s documented policy and procedures include the following policies and if so are they in line with the BSE requirements?   * Information Security Policy * Password Policy * Network Security Policy * Application Software Policy * Backup Policy (data should be available for minimum 5 years) * Audit Trail Policy (data should be available for minimum 5 years)     Whether all the documents are classified as per CIA (Confidentiality, Integrity and Availability)  Does the organization follow any other policy or procedures or documented practices that are relevant? | Results | Opinions |
| **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   * Gateway / Database Server / web server * ETI / AT router * Network Switch | Results | Opinions |
| **Firewall** | Is a firewall implemented?    Are all 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?  Is specific port/service access granted on firewall by following a proper approval process? | Results | Opinions |
| **Physical Security** | Physical Access Control  Server Room/Network Room Security (Environmental Controls)  Server Room/Network Room Security (UPS)  Server Room/Network Room Security (HVAC) | Results | Opinions |

**Declaration:**

There is no conflict of interest with respect to the member being audited and our directors / promoters are not directly or indirectly related to the current directors or promoters of the member being audited.

Signature

(Name of the Auditor & Auditing firm)

CISA / DISA / CISM / CISSP Reg. No :

Date:

Place:

Stamp/Seal:

**Internet Based Trading (IBT)**

**(To be on the letterhead of the system auditor, all pages to be duly stamped and signed)**

**BSE Trading Member Code:**

**BSE Trading Member Name:**

**Areas of Audit:**

* Risk Management
* Security Policy and implementation
* Capacity Management
* Disaster Recovery and Backups
* Vulnerability Test

The detailed findings will be grouped under the above broad categories and classified as ‘Strong’, ‘Medium’ or ‘Weak’ and overall audit rating will be given**.**

| **Controls / Processes** | **Test Case** | **Results, Observations & Control Risk** | **Auditor’s Risk** |
| --- | --- | --- | --- |
| **Location Confirmation**  **The installed IBT system features are as prescribed by the BSE.**  **The installed ETI system parameters are as per BSE norms** | Whether order routing server for IBT is located in India  System network and Network Diagram  Risk Management Tools  Should allow for risk management of the orders placed and online risk monitoring of the orders being placed.  IBT Version   * Order Gateway Version * Risk Administration / Manager Version * Front End / Order Placement Version | Results | Opinions |
| **Trading Process**  **The installed IBT system allows for placing of trades only for authorized clients**  **Risk Management**  **The installed IBT system is capable of assessing the risk of the client as soon as the order comes in and informs the client of acceptance/rejection of the order within a reasonable period.**  **Order /Trade Limit Controls**  **The installed IBT system provides a system based control facility on the trading limits of the clients and exposures taken by the clients including set pre-defined limits on the exposure and turnover of each client.**  **Order Reconfirmation Facility**  **The installed IBT system provides for reconfirmation of orders which are larger than that as specified by the member’s risk management system.**  **Execution of Orders / Order Logic**  **The installed IBT system provides a system based control facility over the order input process** | Client ID Verification  Only duly authorized client’s orders are allowed to be placed.  Order Parameters based on the respective risk profile of the client  There is online risk assessment of all orders placed through the IBT system with following checks :   * Order Value per order should not exceed as specified in RMS (not exceeding the maximum limit as specified by Exchange) * Order Quantity per order should not exceed as specified in RMS * Spread order value and quantity limit per order should not exceed as specified in RMS. * Cumulative value of all unexecuted / open orders should not exceed as specified in RMS at client level * Order value limit at client level * Order value limit at branch level * Security-wise order limits at client level   Only orders that are within the parameters specified by the risk management systems are allowed to be placed  The system has a manual override facility for allowing orders that do not fit the system based risk control parameters  Order Numbering Methodology  If the system is enabled for internet trading the system has an internal unique order numbering system  Order Matching  The system does not have any order matching function and all orders are passed on to the exchange trading system for matching | Results | Opinions |
| **Application Access Control**  **The installed IBT system provides a system based access control over the IBT server as well as the risk management and front end dealing applications while providing for security**  **Session Security**  **The installed IBT system provides for session security for all sessions established with the IBT server by the front end application.**  **Database Security**  **The installed IBT system has sufficient controls over the access to and integrity of the database**  **Encryption**  **The installed IBT system uses confidentiality protection measures to ensure session confidentiality.** | Access controls   * The system allows access to only authorized users * The system has a password mechanism which restricts access to authenticate users.   Session Security   * The system uses session identification and authentication measures to restrict sessions to authorized user only. * The system uses session security measures like encryption to ensure confidentiality of sessions initiated.   Database Security   * The access to the IBT database is allowed only to authorized users / applications. * The IBT database is hosted on a secure platform. * The IBT database stores the user names / passwords securely.   Session Encryption   * The system uses SSL or similar session confidentiality protection mechanisms * The system uses a secure storage mechanism for storing of usernames and passwords. * The system adequately protects the confidentiality of the user’s trade data. | Results | Opinions |
| **The installed IBT 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 IBT systems has a provision for off line monitoring and risk management as per the requirements of BSE and includes reports / logs on   * Number of Authorized Users * Activity logs * Systems logs * Number of active clients |  |  |
| **The installed IBT system Authentication mechanism is as per the guidelines of the BSE** | The installed IBT system’s uses passwords for authentication.  The password policy / standard are documented.  The system requests for identification and new password before login into the system.  The installed IBT system’s Password features include   * The Password is masked at the time of entry. * System mandated changing of password when the user logs in for the first time. * Automatic disablement of the user on entering erroneous password on three consecutive occasions. * Automatic expiry of password on expiry of reasonable period of time as determined by member * 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 password * 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 reasonable minimum length (and no arbitrary maximum length cap or character class). * System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time. | Results | Opinions |
| **The Installed IBT systems backup capability is adequate as per the requirements of the BSE for overcoming loss of product integrity.** | Are backups of the following system generated files maintained as per the BSE guidelines?   * At the IBT server/gateway level * Database * Audit Trails * Reports   At the IBT user level   * Market Watch * Logs * History * Reports * Audit Trails   Are backup procedures documented?  Are backup logs maintained?  Have 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? | Results | Opinions |
| **The installed IBT system features are as prescribed by the BSE.**  **The installed IBT system parameters are as per BSE norms** | 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  Gateway Parameters   * Trader ID   Market Segment   * IP Address * (BSE Network) * VSAT ID * Leased Line ID |  |  |
| **Execution of Orders / Order Logic**  **The installed IBT system provides a system based control facility over the order input process**                          **Trades Information**  **The installed IBT system provides a system based control facility over the trade confirmation process**      **Settlement of Trades**  **The installed IBT system provides a system based reports on contracts, margin requirements, payment and delivery obligations** | 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.      Trade Confirmation and Reporting Feature  Should allow confirmation and reporting of the orders that have resulted in trade        Margin Reports feature  Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | Results | Opinions |
| **To ensure information security for the Organisation in general and the installed IBT system in particular policy and procedures as per the BSE 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 BSE requirements?   * Information Security Policy * Password Policy * Network Security Policy * Application Software Policy * Backup Policy * Audit Trail Policy     Does the organisation follow any other policy or procedures or documented practices that are relevant? | Results | Opinions |
| **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   * Gateway / Database Server / web server * ETI router * Network Switch |  |  |
| **Firewall** | Is a firewall implemented?  Are all 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?  Is specific port/service access granted on firewall by following a proper approval process? |  |  |
| **Physical Security** | Physical Access Control  Server Room/Network Room Security  (Environmental Controls)  Server Room/Network Room Security  (UPS)  Server Room/Network Room Security  (HVAC) |  |  |

**Declaration:**

There is no conflict of interest with respect to the member being audited and our directors / promoters are not directly or indirectly related to the current directors or promoters of the member being audited.

Signature

(Name of the Auditor & Auditing firm)

CISA / DISA / CISM / CISSP Reg. No :

Date:

Place:

Stamp/Seal:

**Direct Market Access (DMA)**

**(To be on the letterhead of the system auditor, all pages to be duly stamped and signed)**

**BSE Trading Member Code:**

**BSE Trading Member Name:**

**Areas of Audit:**

* Risk Management
* Security Policy and implementation
* Capacity Management
* Disaster Recovery and Backups
* Vulnerability Test

The detailed findings will be grouped under the above broad categories and classified as ‘Strong’, ‘Medium’ or ‘Weak’ and overall audit rating will be given**.**

| **Controls / Processes** | **Test Case** | **Results, Observations & Control Risk** | **Auditor’s Risk** |
| --- | --- | --- | --- |
| **Location Confirmation**  **The installed DMA system features are as prescribed by the BSE.**  **The installed ETI system parameters are as per BSE norms** | Whether order routing server for DMA is located in India System network and Network Diagram  Risk Management Tools  Should allow for risk management of the orders placed and online risk monitoring of the orders being placed.  DMA Version   * Order Gateway Version * Risk Administration / Manager Version | Results | Opinions |
| **Trading Process**  **The installed DMA system allows for placing of trades only for authorized clients**  **Risk Management**  **The installed DMA system is capable of assessing the risk of the client as soon as the order comes in and informs the client of acceptance/rejection of the order within a reasonable period.**  **Order /Trade Limit Controls**  **The installed DMA system provides a system based control facility on the trading limits of the clients and exposures taken by the clients including set pre-defined limits on the exposure and turnover of each client.**  **Order Reconfirmation Facility**  **The installed DMA system provides for reconfirmation of orders which are larger than that as specified by the member’s risk management system.**  **Execution of Orders / Order Logic**  **The installed DMA system provides a system based control facility over the order input process** | Client ID / User id Verification  Only duly authorized client’s orders are allowed to be placed.  Order Parameters based on the respective risk profile of the client  There is online risk assessment of all orders placed through the DMA system with following checks :   * Order Value per order should not exceed as specified in RMS (not exceeding the maximum limit as specified by Exchange) * Order Quantity per order should not exceed as specified in RMS * Spread order value and quantity limit per order should not exceed as specified in RMS. * Cumulative value of all unexecuted / open orders should not exceed as specified in RMS at client level * Order value limit at client level * Order value limit at branch level * Security-wise order limits at client level   Only orders that are within the parameters specified by the risk management systems are allowed to be placed.  Are there provisions for setting trading limits, exposure limits, position limits, order quantity limits order value limits, price range checks, Net Position limits for all DMA clients based on risk assessment, credit quality and available margins of the client. Also appropriate limits for securities which are subject to FII limits as specified as RBI.  The system has a manual override facility for allowing orders that do not fit the system based risk control parameters  Order Numbering Methodology  If the system is enabled for DMA the system has an internal unique order numbering system  Order Matching  The system does not have any order matching function resulting into cross trades of the clients orders of a trading member with each other. All orders are passed on to the exchange trading system for matching.  Whether Broker is using similar logic/ priorities as used by Exchange to treat DMA client orders.  Whether DMA orders are having unique flag/ tag as specified by the Exchange. | Results | Opinions |
| **Application Access Control**  **The installed DMA system provides a system based access control over the DMA server as well as the risk management and front end dealing applications while providing for security**  **Session Security**  **The installed DMA system provides for session security for all sessions established with the DMA server by the front end application.**  **Database Security**  **The installed DMA system has sufficient controls over the access to and integrity of the database**  **Encryption**  **The installed DMA system uses confidentiality protection measures to ensure session confidentiality.** | Access controls   * The system allows access to only authorized users * The system has appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager * The system has a password mechanism which restricts access to authenticate users.   Session Security   * The system uses session identification and authentication measures to restrict sessions to authorized user only. * The system uses session security measures like encryption to ensure confidentiality of sessions initiated.   Database Security   * The access to the DMA database is allowed only to authorized users / applications. * The DMA database is hosted on a secure platform. * The DMA database stores all the details of user ids activated for DMA along with user names and passwords securely. * Frequency of antivirus patch updation   Session Encryption   * The system uses session confidentiality protection mechanisms * The system uses a secure storage mechanism for storing of usernames and passwords. * The system adequately protects the confidentiality of the users’ trade data. | Results | Opinions |
| **The installed DMA 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 DMA system has a provision for off line monitoring and risk management as per the requirements of BSE and includes reports / logs on   * Number of Authorized Users * Activity logs * Systems logs * Number of active clients * Review of logs (activity/system/alert/incident) |  |  |
| **The installed DMA system Authentication mechanism is as per the guidelines of the BSE** | The installed DMA system’s uses passwords for authentication.  The password policy / standard are documented.  The system requests for identification and new password before login into the system.  The installed DMA system’s Password features include   * The Password is masked at the time of entry. * System mandated changing of password when the user logs in for the first time. * Automatic disablement of the user on entering erroneous password on three consecutive occasions. * Automatic expiry of password on expiry of reasonable period of time as determined by member * 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 password * 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 reasonable minimum length (and no arbitrary maximum length cap or character class). * System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time. * System control ensures Re-initialisation of access on entering fresh passwords. | Results | Opinions |
| **The Installed DMA systems backup capability is adequate as per the requirements of the BSE for overcoming loss of product integrity.** | Are backups of the following system generated files maintained as per the BSE guidelines?   * At the DMA server/gateway level * Database * Audit Trails * Reports   At the DMA user level   * Market Watch * Logs * History * Reports * Audit Trails * Alert logs   Are backup procedures documented?  Are backup logs maintained?  Have 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? | Results | Opinions |
| **The installed DMA system parameters are as per BSE norms** | Gateway Parameters   * Trader ID   Market Segment   * IP Address * (BSE Network) * VSAT ID * Leased Line ID |  |  |
| **Trades Information**  **The installed DMA system provides a system based control facility over the trade confirmation process**      **Settlement of Trades**  **The installed DMA system provides a system based reports on contracts, margin requirements, payment and delivery obligations** | Trade Confirmation and Reporting Feature  Should allow confirmation and reporting of the orders that have resulted in trade        Margin Reports feature  Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | Results | Opinions |
| **To ensure information security for the Organization in general and the installed DMA system in particular policy and procedures as per the BSE requirements must be established, implemented and maintained.** | Systems & procedures:  Whether installed systems & procedures are adequate to handle DMA orders/ trades?  Maintenance of User details:  Whether details of users activated for DMA facilities is maintained along with user name, unique identification of user, authorization levels.  Does the organization’s documented policy and procedures include the following policies and if so are they in line with the BSE requirements?   * Information Security Policy * Password Policy * Network Security Policy * Application Software Policy * Backup Policy (data should be available for minimum 5 years) * Audit Trail Policy (data should be available for minimum 5 years)     Whether all the documents are classified as per CIA (Confidentiality, Integrity and Availability)  Does the organization follow any other policy or procedures or documented practices that are relevant? | Results | Opinions |
| **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   * Gateway / Database Server / web server * ETI router * Network Switch | Results | Opinions |
| **Firewall** | Is a firewall implemented?    Are all 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?  Is specific port/service access granted on firewall by following a proper approval process? | Results | Opinions |
| **Physical Security** | Physical Access Control  Server Room/Network Room Security (Environmental Controls)  Server Room/Network Room Security (UPS)  Server Room/Network Room Security (HVAC) | Results | Opinions |

**Declaration:**

There is no conflict of interest with respect to the member being audited and our directors / promoters are not directly or indirectly related to the current directors or promoters of the member being audited.

Signature

(Name of the Auditor & Auditing firm)

CISA / DISA / CISM / CISSP Reg. No :

Date:

Place:

Stamp/Seal:

**Securities Trading using Wireless Technology (STWT)**

**(To be on the letterhead of the system auditor, all pages to be duly stamped and signed)**

**BSE Trading Member Code:**

**BSE Trading Member Name:**

**Areas of Audit:**

* Risk Management
* Security Policy and implementation
* Capacity Management
* Disaster Recovery and Backups
* Vulnerability Test

The detailed findings are required to be grouped under the above broad categories and classified as ‘Strong’, ‘Medium’ or ‘Weak’ and overall audit rating is required to be given**.**

| **Controls / Processes** | **Test Case** | **Results, Observations & Control Risk** | **Auditor’s Risk** |
| --- | --- | --- | --- |
| **Location Confirmation**  **The installed STWT system features are as prescribed by the BSE.**  **The installed ETI system parameters are as per BSE norms** | Whether order routing server for STWT is located in India System network and Network Diagram  Risk Management Tools   * Should allow for risk management of the orders placed and online risk monitoring of the orders being placed.   STWT Version   * Order Gateway Version * Risk Administration / Manager Version * Front End / Order Placement Version | Results | Opinions |
| **Trading Process**  **The installed STWT system allows for placing of trades only for authorized clients**  **Risk Management**  **The installed STWT system is capable of assessing the risk of the client as soon as the order comes in and informs the client of acceptance/rejection of the order within a reasonable period.**  **Order /Trade Limit Controls**  **The installed STWT system provides a system based control facility on the trading limits of the clients and exposures taken by the clients including set pre-defined limits on the exposure and turnover of each client.**  **Order Reconfirmation Facility**  **The installed STWT system provides for reconfirmation of orders which are larger than that as specified by the member’s risk management system.**  **Execution of Orders / Order Logic**  **The installed STWT system provides a system based control facility over the order input process** | Client ID Verification  Only duly authorized client’s orders are allowed to be placed.  Order Parameters based on the respective risk profile of the client  There is online risk assessment of all orders placed through the STWT system with following checks :   * Order Value per order should not exceed as specified in RMS (not exceeding the maximum limit as specified by Exchange) * Order Quantity per order should not exceed as specified in RMS * Spread order value and quantity limit per order should not exceed as specified in RMS. * Cumulative value of all unexecuted / open orders should not exceed as specified in RMS at client level * Order value limit at client level * Order value limit at branch level * Security-wise order limits at client level   Only orders that are within the parameters specified by the risk management systems are allowed to be placed  The system has a manual override facility for allowing orders that do not fit the system based risk control parameters  Order Numbering Methodology  If the system is enabled for securities trading using wireless technology the system has an internal unique order numbering system  Order Matching  The system does not have any order matching function and all orders are passed on to the exchange trading system for matching  Whether Broker is using similar logic/ priorities as used by Exchange to treat STWT client orders.  Whether STWT orders are having unique flag/ tag as specified by the Exchange. | Results | Opinions |
| **Application Access Control**  **The installed STWT system provides a system based access control over the STWT server as well as the risk management and front end dealing applications while providing for security**  **Session Security**  **The installed STWT system provides for session security for all sessions established with the STWT server by the front end application.**  **Database Security**  **The installed STWT system has sufficient controls over the access to and integrity of the database**  **Encryption**  **The installed STWT system uses confidentiality protection measures to ensure session confidentiality.** | Access controls   * The system allows access to only authorized users using means such as user-id, passwords, smart cards, biometric devices or other reliable means * The system has a password mechanism which restricts access to authenticate users.   Session Security   * The system uses session identification and authentication measures to restrict sessions to authorized user only. * The system uses session security measures like encryption to ensure confidentiality of sessions initiated. * Session login details should not be stored on the devices used for STWT.   Database Security   * The access to the STWT database is allowed only to authorized users / applications. * The STWT database is hosted on a secured platform. * The STWT database stores the user names / passwords securely.   Session Encryption   * The system uses SSL or similar session confidentiality protection mechanisms * The system uses a secure storage mechanism for storing of usernames and passwords. * The system adequately protects the confidentiality of the users’ trade data. | Results | Opinions |
| **The installed STWT 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 STWT systems has a provision for off line monitoring and risk management as per the requirements of BSE and includes reports / logs on   * Number of Authorized Users * Activity logs * Systems logs * Number of active clients | Results | Opinions |
| **The installed STWT system Authentication mechanism is as per the guidelines of the BSE** | The installed STWT system uses passwords for authentication.  The password policy / standard are documented.  The system requests for identification and new password before login into the system.  The installed STWT system’s Password features include :   * The Password is masked at the time of entry. * System mandated changing of password when the user logs in for the first time. * Automatic disablement of the user on entering erroneous password on three consecutive occasions. * Automatic expiry of password on expiry of reasonable period of time as determined by member * 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 password * 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 reasonable minimum length (and no arbitrary maximum length cap or character class). * System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time. | Results | Opinions |
| **The Installed STWT systems backup capability is adequate as per the requirements of the BSE for overcoming loss of product integrity.** | Are backups of the following system generated files maintained as per the BSE guidelines?   * At the STWT server/gateway level * Database * Audit Trails * Reports   At the STWT user level   * Market Watch * Logs * History * Reports * Audit Trails   Are backup procedures documented?  Are backup logs maintained?  Have 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? | Results | Opinions |
| **The installed STWT system features are as prescribed by the BSE.**  **The installed STWT system parameters are as per BSE norms** | 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   Website address for detailed information   * The system provides address of the web site/web page where detailed information of order / trades would be available.   Gateway Parameters   * Trader ID   Market Segment   * IP Address * (BSE Network) * VSAT ID * Leased Line ID | Results | Opinions |
| **Execution of Orders / Order Logic**  **The installed STWT system provides a system based control facility over the order input process**                          **Trades Information**  **The installed STWT system provides a system based control facility over the trade confirmation process**    **Settlement of Trades**  **The installed STWT system provides a system based reports on contracts, margin requirements, payment and delivery obligations** | 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.     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    Margin Reports feature  Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | Results | Opinions |
| **To ensure information security for the Organization in general and the installed STWT system in particular policy and procedures as per the BSE 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 BSE requirements?   * Information Security Policy * Password Policy * Network Security Policy * Application Software Policy * Backup Policy * Audit Trail Policy     Does the organisation follow any other policy or procedures or documented practices that are relevant? | Results | Opinions |
| **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   * Gateway / Database Server / web server * ETI router * Network Switch | Results | Opinions |
| **Firewall** | Is a firewall implemented?  Are all 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?  Is specific port/service access granted on firewall by following a proper approval process? | Results | Opinions |
| **Physical Security** | Physical Access Control  Server Room/Network Room Security (Environmental Controls)  Server Room/Network Room Security (UPS)  Server Room/Network Room Security (HVAC) | Results | Opinions |

**Declaration:**

There is no conflict of interest with respect to the member being audited and our directors / promoters are not directly or indirectly related to the current directors or promoters of the member being audited.

Signature

(Name of the Auditor & Auditing firm)

CISA / DISA / CISM / CISSP Reg. No :

Date:

Place:

Stamp/Seal:

**Smart Order Routing (SOR)**

**(To be on the letterhead of the system auditor, all pages to be duly stamped and signed)**

**BSE Trading Member Code:**

**BSE Trading Member Name:**

**Areas of Audit:**

* Risk Management
* Security Policy and implementation
* Capacity Management
* Disaster Recovery and Backups
* Vulnerability Test

The detailed findings will be grouped under the above broad categories and classified as ‘Strong’, ‘Medium’ or ‘Weak’ and overall audit rating will be given**.**

| **Controls / Processes** | **Test Case** | **Results, Observations & Control Risk** | **Auditor’s Risk** |
| --- | --- | --- | --- |
| **Location Confirmation**  **The installed SOR system features are as prescribed by the BSE.**  **The installed ETI system parameters are as per BSE norms** | Whether order routing server for SOR is located in India System network and Network Diagram  Risk Management Tools  Should allow for risk management of the orders placed and online risk monitoring of the orders being placed.  SOR Version   * Order Gateway Version * Risk Administration / Manager Version | Results | Opinions |
| **Trading Process**  **The installed SOR system allows for placing of Orders only for authorized clients**  **Risk Management**  **The installed SOR system is capable of assessing the risk of the client as soon as the order comes in and informs the client of acceptance/rejection of the order within a reasonable period.**  **Market Data Feed**  **The market data feed integrated to the SOR system are received directly from the recognized Stock Exchanges**  **Order /Trade Limit Controls**  **The installed SOR system provides a system based control facility on the trading limits of the clients and exposures taken by the clients including set pre-defined limits on the exposure and turnover of each client.**  **Order Reconfirmation Facility**  **The installed SOR system provides for reconfirmation of orders which are larger than that as specified by the member’s risk management system.**  **Execution of Orders / Order Logic**  **The installed SOR system provides a system based control facility over the order input process** | Client ID / User id Verification  Only duly authorized client’s orders are allowed to be placed.  SOR facility is provided to all class of investors  Order Parameters based on the respective risk profile of the client  There is online risk assessment of all orders placed through the SOR system with following checks :   * Order Value per order should not exceed as specified in RMS (not exceeding the maximum limit as specified by Exchange) * Order Quantity per order should not exceed as specified in RMS * Spread order value and quantity limit per order should not exceed as specified in RMS. * Cumulative value of all unexecuted / open orders should not exceed as specified in RMS at client level * Order value limit at client level * Order value limit at branch level * Security-wise order limits at client level   Market Data Feed  The market prices are received directly from recognized stock Exchanges and are time stamped  The market prices of all the recognized stock exchanges to which the SOR facility routes orders are consolidated for applying the Best Execution Policy for routing orders  Only orders that are within the parameters specified by the risk management systems are allowed to be placed.  Are there provisions for setting trading limits, exposure limits, position limits, order quantity limits order value limits, price range checks, Net Position limits for all SOR clients based on risk assessment, credit quality and available margins of the client. Also appropriate limits for securities which are subject to FII limits as specified as RBI.  The system has a manual override facility for allowing orders that do not fit the system based risk control parameters  Order Numbering Methodology  If the system is enabled for SOR the system has an internal unique order numbering system  Order Matching  The SOR system adheres to the Best Execution Policy while routing the orders to the exchange.  The SOR system routes orders to the recognized stock exchanges in a neutral manner  The system provides functionality for the client who has availed of the SOR facility to specify for individual orders for which they do not want to route the order using SOR facility  The SOR system does not release orders to venues other than the recognized stock Exchange (Specify the list of recognized Stock Exchange(s) and the market segments to which SOR release orders)  The system does not have any order matching function resulting into cross trades of the clients orders of a trading member with each other. All orders are passed on to the exchange trading system for matching.  Whether Broker is using similar logic/ priorities as used by Exchange to treat SOR client orders.  Whether SOR orders are having unique flag/ tag as specified by the Exchange. | Results | Opinions |
| **Application Access Control**  **The installed SOR system provides a system based access control over the SOR server as well as the risk management and front end dealing applications while providing for security**  **Session Security**  **The installed SOR system provides for session security for all sessions established with the SOR server by the front end application.**  **Database Security**  **The installed SOR system has sufficient controls over the access to and integrity of the database**  **Encryption**  **The installed SOR system uses confidentiality protection measures to ensure session confidentiality.** | Access controls   * The system allows access to only authorized users * The system has appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager * The system has a password mechanism which restricts access to authenticate users.   Session Security   * The system uses session identification and authentication measures to restrict sessions to authorized user only. * The system uses session security measures like encryption to ensure confidentiality of sessions initiated.   Database Security   * The access to the SOR database is allowed only to authorized users / applications. * The SOR database is hosted on a secure platform. * The SOR database stores all the details of user ids activated for SOR along with user names and passwords securely. * Frequency of antivirus patch updation   Session Encryption   * The system uses session confidentiality protection mechanisms * The system uses a secure storage mechanism for storing of usernames and passwords. * The system adequately protects the confidentiality of the users’ trade data. | Results | Opinions |
| **The installed SOR 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 SOR system has a provision for off line monitoring and risk management as per the requirements of BSE and includes reports / logs on   * Number of Authorized Users * Activity logs * Systems logs * Number of active clients * Review of logs (activity/system/alert/incident) |  |  |
| **The installed SOR system Authentication mechanism is as per the guidelines of the BSE** | The installed SOR system’s uses passwords for authentication.  The password policy / standard are documented.  The system requests for identification and new password before login into the system.  The installed SOR system’s Password features include   * The Password is masked at the time of entry. * System mandated changing of password when the user logs in for the first time. * Automatic disablement of the user on entering erroneous password on three consecutive occasions. * Automatic expiry of password on expiry of reasonable period of time as determined by member * 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 password * 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 reasonable minimum length (and no arbitrary maximum length cap or character class). * System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time. * System control ensures Re-initialisation of access on entering fresh passwords. | Results | Opinions |
| **The Installed SOR systems backup capability is adequate as per the requirements of the BSE for overcoming loss of product integrity.** | Are backups of the following system generated files maintained as per the BSE guidelines?   * At the SOR server/gateway level * Database * Audit Trails * Reports   At the SOR user level   * Market Watch * Logs * History * Reports * Audit Trails * Alert logs   Does the audit trail capture the record of orders, trades and data points for the basis of routing decision?  Are backup procedures documented?  Are backup logs maintained?  Have 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? | Results | Opinions |
| **The installed SOR system parameters are as per BSE norms** | Gateway Parameters   * Trader ID   Market Segment   * IP Address * (BSE Network) * VSAT ID * Leased Line ID |  |  |
| **Trades Information**  **The installed SOR system provides a system based control facility over the trade confirmation process**    **Settlement of Trades**  **The installed SOR system provides a system based reports on contracts, margin requirements, payment and delivery obligations** | Trade Confirmation and Reporting Feature  Should allow confirmation and reporting of the orders that have resulted in trade      Margin Reports feature  Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | Results | Opinions |
| **To ensure information security for the Organization in general and the installed SOR system in particular policy and procedures as per the BSE requirements must be established, implemented and maintained.** | Systems & procedures:  Whether installed systems & procedures are adequate to handle SOR orders/ trades?  Maintenance of User details:  Whether details of users activated for SOR facilities is maintained along with user name, unique identification of user, authorization levels.  Does the organization’s documented policy and procedures include the following policies and if so are they in line with the BSE requirements?   * Information Security Policy * Password Policy * Network Security Policy * Application Software Policy * Backup Policy (data should be available for minimum 5 years) * Audit Trail Policy (data should be available for minimum 5 years)     Whether all the documents are classified as per CIA (Confidentiality, Integrity and Availability)  Does the organization follow any other policy or procedures or documented practices that are relevant? | Results | Opinions |
| **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   * Gateway / Database Server / web server * ETI router * Network Switch | Results | Opinions |
| **Firewall** | Is a firewall implemented?  Are all 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?  Is specific port/service access granted on firewall by following a proper approval process? | Results | Opinions |
| **Physical Security** | Physical Access Control  Server Room/Network Room Security (Environmental Controls)  Server Room/Network Room Security (UPS)  Server Room/Network Room Security (HVAC) | Results | Opinions |

**Declaration:**

There is no conflict of interest with respect to the member being audited and our directors / promoters are not directly or indirectly related to the current directors or promoters of the member being audited.

Signature

(Name of the Auditor & Auditing firm)

CISA / DISA / CISM / CISSP Reg. No :

Date:

Place:

Stamp/Seal: