Internet Based Trading (IBT) - System Audit Report

For

**234**

**(Trading Member Code 324)**

For



Authored By



March 3, 2025

|  |
| --- |
| The information in this document has been classified as “**Confidential**”. This classification applies to the most sensitive business information, which is intended strictly for use within **234** and **National Stock Exchange of India Limited**. Its unauthorized disclosure could seriously and adversely impact the owner, its stakeholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion. |

#### **NSE Trading Code: member\_code**

#### **NSE Trading Member Name: 234**

1. **Area Of Audit:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Category** | **Strong** | **Medium** | **Weak** |
| Risk Management |  |  |  |
| Security Policy and Implementation |  |  |  |
| Capacity Management |  |  |  |
| Disaster Recovery & backups |  |  |  |
| Vulnerability Tests |  |  |  |

1. **Overall rating**

# Based on our assessment of the risks the systems face and the tests of the operating effectiveness of the controls developed by the member to alleviate those risks, Overall Rating was found to be STRONG.

1. **Detailed Observations**

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls / Processes** | **Test Case** | **Results, Observations & Control Risk** | **Auditor’s Risk** |
| **Location Confirmation** | Whether order routing server for IBT is located in India | 234 |  |
| **The installed IBT system features are as prescribed by the NSE.** | System network and Network Diagram | 234 |  |
| Risk Management Tools  Should allow for risk management of the orders placed and online risk monitoring of the orders being placed. | A pre-defined trading limit can be set for each client in the 234 which performs the online risk assessment for each order | Strong |
| **The installed CTCL system parameters are as per NSE norms** | IBT Version   * Order Gateway Version * Risk Administration / Manager Version * Front End / Order Placement Version | * 234 * 234 * 234 |  |
| **Trading Process**  **The installed IBT system allows for placing of trades only for authorized clients** | Client ID Verification  Only duly authorized client’s orders are allowed to be placed. | Only duly authorized client’s orders are allowed to be placed through specific user-ids. | Strong |
| **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 Parameters  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 | A pre-defined trading limit can be set for each client in the 234, which performs the online risk assessment for each order.  A provision exists to monitor all orders for the following parameters:   * Order Value per order * Order Quantity per order * Spread order value and quantity limit per order * Cumulative value of all unexecuted / open orders * Order value limit at client level * Order value limit at branch level * Security-wise order limits at client level | Strong |
| **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.** | Only orders that are within the parameters specified by the risk management systems are allowed to be placed. | A pre-defined trading limit can be set for each client in the 234, which performs the online risk assessment for each order. | Strong |
| **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.** | The system has a manual override facility for allowing orders that do not fit the system-based risk control parameters | Within the system a facility for overriding orders that do not fit the risk control parameters was not observed.  The client would be required to enter a new order after an order is rejected by the RMS system. | Strong |
| **Execution of Orders / Order Logic**  **The installed IBT system provides a system-based control facility over the order input process** | Order Numbering Methodology  If the system is enabled for internet trading the system has an internal unique order numbering system | Compliant | Strong |
| Order Matching  The system does not have any order matching function and all orders are passed on to the exchange trading system for matching. | Compliant | Strong |
| **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** | Access controls   1. The system allows access to only authorized users | Compliant | Strong |
| 1. The system has a password mechanism which restricts access to authenticate users. | Compliant | Strong |
| **Session Security**  **The installed IBT system provides for session security for all sessions established with the IBT server by the front-end application.** | Session Security   * The system uses session identification and authentication measures to restrict sessions to authorized user only. | Compliant | Strong |
| * The system uses session security measures like encryption to ensure confidentiality of sessions initiated. | Compliant | Strong |
| **Database Security**  **The installed IBT system has sufficient controls over the access to and integrity of the database** | Database Security   * The access to the IBT database is allowed only to authorized users / applications. | Compliant | Strong |
| * The IBT database is hosted on a secure platform. | Compliant | Strong |
| * The IBT database stores the user names / passwords securely. | Compliant | Strong |
| **Encryption**  **The installed IBT system uses confidentiality protection measures to ensure session confidentiality.** | Session Encryption  The system uses SSL or similar session confidentiality protection mechanisms | Compliant | Strong |
| The system uses a secure storage mechanism for storing of usernames and passwords. | Compliant | Strong |
| The system adequately protects the confidentiality of the users’ trade data. | Compliant | Strong |
| **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 system has a provision for off line monitoring and risk management as per the requirements of NSE and includes reports / logs on | Compliant | Strong |
| Number of Authorized Users | Compliant |
| Activity logs | Compliant |
| Systems logs | Compliant |
| Number of active clients | Compliant |
| **The installed IBT system Authentication mechanism is as per the guidelines of the NSE** | The installed IBT system’s uses passwords for authentication. | Compliant | Strong |
| The password policy / standard is documented. | Compliant | Strong |
| The system requests for identification and new password before login into the system. | Compliant | Strong |
| The installed IBT system’s Password features include: | - | Strong |
| * The Password is masked at the time of entry. | Compliant |
| * System mandated changing of password when the user logs in for the first time. | Compliant |
| * Automatic disablement of the user on entering erroneous password on three consecutive occasions. | Compliant |
| * Automatic expiry of password on expiry of reasonable period of time as determined by member | Compliant |
| * System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical. | Compliant |
| * System controls to ensure that the changed password cannot be the same as of the last password. | Compliant |
| * System controls to ensure that the Login id of the user and password should not be the same. | Compliant |
| * System controls to ensure that the Password should be of reasonable minimum length (and no arbitrary maximum length cap or character class). | Compliant |
| * 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. | Compliant |
| **The Installed IBT systems backup capability is adequate as per the requirements of the NSE for overcoming loss of product integrity.** | Are backups of the following system generated files maintained as per the NSE guidelines? |  |  |
| At the IBT server / gateway level | Compliant | Strong |
| * Database |
| * Audit Trails |
| * Reports |
| At the IBT user level | Compliant | Strong |
| * Market Watch |
| * Logs |
| * History |
| * Reports |
| * Audit Trails |
| Are backup procedures documented? | Compliant | Strong |
| Are backup logs maintained? | Compliant | Strong |
| Have the backups been verified and tested? | Compliant | Strong |
| Are the backup media stored safely in line with the risk involved? | Compliant | Strong |
| Are there any recovery procedures and have the same been tested? | Compliant | Strong |
| **The installed IBT system features are as prescribed by the NSE.** | Main Features Price Broadcast  The system has a feature for receipt of price broadcast data | Compliant | Strong |
| Order Processing: The system has a feature:   1. Which allows order entry and confirmation of orders. 2. which allows for modification or cancellation of orders placed | Compliant | Strong |
| Trade Confirmation  The system has a feature which enables confirmation of trades | Compliant | Strong |
| **The installed IBT system parameters are as per NSE norms** | Gateway Parameters   * Trader ID | 243 |  |
| **Market Segment –** | 234\_name |
| * IP Address | 234 |
| * (NSE Network) | - |
| * VSAT ID | - |
| * Leased Line ID | 234 |
| **Execution of Orders / Order Logic**  **The installed IBT system provides a system-based control facility over the order input process** | Order Entry  The system has order placement controls that allow only orders matching the system parameters to be placed. | Compliant | Strong |
| Order Modification  The system allows for modification of orders placed. | Order modification features are present at the  234 allowing order modification capabilities for pending orders only.  The system also provides modification facilities for Quantity, Price, Type and Validity to the users.  But the user or administrator cannot modify executed orders. |  |
| Order Cancellation  The system allows for cancellation of orders placed | Compliant | Strong |
| 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. | Compliant | Strong |
| **Trades Information**  **The installed IBT system provides a system-based control facility over the trade confirmation process** | Trade Confirmation and Reporting Feature  Should allow confirmation and reporting of the orders that have resulted in trade | Compliant | Strong |
| **Settlement of Trades**  **The installed IBT system provides a system-based reports on contracts, margin requirements, payment & delivery obligations** | Margin Reports feature  Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | Compliant | Strong |
| **To ensure information security for the Organization in general and the installed IBT system in particular policy and procedures as per the NSE 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 NSE requirements? | Documented policies were verified. | Strong |
| * Information Security Policy | Compliant | Strong |
| * Password Policy | Compliant |
| * Network Security Policy | Compliant |
| * Application Software Policy | Compliant |
| * Backup Policy | Compliant |
| * Audit Trail Policy | Compliant |
| Does the organization follow any other policy or procedures or documented practices that are relevant? | Compliant |
| **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 | Compliant | Strong |
| 1. Gateway / Database Server / web server | Compliant |
| 1. CTCL router | Compliant |
| 1. Network Switch | Compliant |
| **Firewall** | Is a firewall implemented? | firewall\_name firewall is implemented. |  |
| Are all servers placed in a DMZ and segregated from other zones by using a firewall? | The web server is implemented within the DMZ separate from the application and database server. | Strong |
| Is there segregation between application and database servers? | The application and database servers are maintained separately. | Strong |
| Are user and server zones segregated? | All the trading servers are hosted within the datacenter within the office of the member. This ensures that the user and server zones are separate. | Strong |
| Is specific port/service access granted on firewall by following a proper approval process? | Yes, Access to specific Port / Service approval in place. Records of approval are maintained via email. | Strong |
| **Physical Security** | Physical Access Control | Automated controls to restrict access to the server room are implemented. Audit Trails of Entry - Exit are maintained. | Strong |
| Server Room / Network Room Security (Environmental Controls) | Environmental controls within the data center were satisfactory | Strong |
| Server Room / Network Room Security (UPS) | UPS and power supply systems were found to be adequate. | Strong |
| Server Room / Network Room Security (HVAC) | UPS and power supply systems were found to be adequate. | Strong |

#### **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.

**For Kochar Consultants Private Limited**

**Kamlesh Kale**

**Head | IT Governance, Risk & Compliance | IT Security**

CISA Certificate No: 20163284

**Kochar Consultants Private Limited**

302, Swapna Bhoomi, A Wing,

S.K. Bole Road, Dadar (W),

Mumbai - 400028.

Tel: 24379537 / 24378212

[info@kocharconsultants.com](mailto:info@kocharconsultants.com)

**Date : 03/03/2025**

**Place: Mumbai**