Centinel Securities Pvt. Ltd.
399, St 58, D-12/2, Islamabad
+92 333 545 9996

CENTINEL SECURITIES (PRIVATE) LIMITED

PAKISTAN STOCK EXCHANGE TRE CERTIFICATE NO. 551

INTERNAL CONTROL & RISK MANAGEMENT FRAMEWORK

S.No.	Detail	Date
1.	Prepared by Compliance Officer	23 June 2025
2.	Reviewed & Approved by CEO	26 June 2025

INTERNAL CONTROL & RISK MANAGEMENT FRAMEWORK

1. POLICY ADHERENCE

All employees, management, and executive leadership at Centinel Securities (Pvt) Ltd. (CSL) are expected to strictly follow this policy. Its effectiveness relies on consistent compliance at every level. Designated personnel will be tasked with reviewing compliance on a quarterly basis and reporting their findings to the CEO or Board of Directors. Any violations or failure to follow this policy may lead to disciplinary measures.

2. POLICY REVIEW

This policy shall be reviewed biennially, or earlier if there are major operational, regulatory, or organizational changes. The review ensures that the policy remains aligned with CSL's strategic direction and operational requirements.

3. STATEMENT OF POLICY

The Board of Directors holds the ultimate responsibility for risk oversight and ensuring that a reliable system of internal controls is in place. CSL is committed to establishing internal control mechanisms that ensure the accuracy and integrity of financial reporting (in line with IFRS), safeguard assets, and promote organizational sustainability.

Relying on input from management and assurance functions, the Board must be able to affirm that the company's internal controls are sound and that financial data can be trusted for reporting purposes. The Board must also confirm that no material control failure has come to their notice that would compromise company operations or result in significant loss.

This document outlines key objectives of internal controls at CSL, defines the roles of the Board, Audit & Risk Committee, management, internal and external auditors, and other control-related functions.

---

4. DEFINITION

Internal Control
A structured process influenced by the Board, management, and employees, aimed at managing risks to support the achievement of company goals in the following areas:

- Operational efficiency and effectiveness
- Accurate and meaningful reporting
- Adherence to applicable laws and regulations
- Protection of assets and resources
- Strengthened corporate governance

---

5. POLICY PURPOSE

Implementing internal controls allows CSL to remain aligned with its strategic goals while managing risks, adapting to changes, and complying with legal obligations. These controls also improve operational efficiency, promote reliable reporting, and encourage compliance across the organization.

The main aims of this policy are to:

- Ensure all published data—internal or external—is timely, correct, and trustworthy
- Verify that all actions by staff and management are in accordance with established laws, standards, and internal policies
- Ensure that organizational resources, systems, and data are appropriately protected
- Support the achievement of strategic and operational goals
- Identify and evaluate potential risks within each business unit
- Foster an environment that requires accountability and performance from all employees and management

CENTINEL SECURITIES (PRIVATE) LIMITED

6. POLICY SCOPE

This policy applies to all permanent, temporary, contract-based employees, as well as management and Board members of CSL, its subsidiaries, and any operational branches.

---

7. GUIDING PRINCIPLES

This policy aims to maintain a consistent and effective internal control environment across CSL. The controls must be uniformly applied to protect the interests of the company and its stakeholders from any financial, operational, or reputational risks.

---

8. SPECIFIC CONTROL AREAS

8.1 Account Opening and KYC/AML Procedures

8.1.1 A dedicated department must maintain records of all new and existing clients, including detailed account opening documentation.

8.1.2 Comprehensive KYC and Customer Due Diligence (CDD) frameworks should address:

- Customer identification
- Verification of income (especially for individuals or sole proprietors)
- Risk profiling of clients
- Criteria for enhanced or simplified due diligence
- Adequate staffing for compliance operations
- Data retention practices
- Management Information System (MIS) reporting capacity
- Ongoing employee training

8.1.3 Required documentation by customer type includes:

Category	Required Documentation
Individuals/Sole Proprietors	CNIC/NICOP, passport (foreign clients), proof of income, employment/business documents, NTN (if applicable), nominee details, mobile ownership proof
Partnerships	CNICs/NICOPs of partners, partnership deed, registration certificate (if applicable), latest financials, NTN
Institutions/Corporates	CNICs/NICOPs of directors and signatories, incorporation documents, board resolution, MoA/AoA/Trust Deed, financial statements
Trusts	CNICs of trustees, trust deed, financials, tax exemption (if applicable)
Clubs, Societies & Associations	CNICs of governing body, registration certificate, bylaws, financials
Executors/Administrators	CNICs of all executors, letter of administration, resolution

---

8.2 Customer Account Opening Controls

8.2.1 Each relevant department must implement effective mechanisms to retain customer identification records and ensure their timely updates.

8.2.2 Senior compliance personnel, preferably the Compliance Officer, must authorize new account openings. A comprehensive checklist of required supporting documents, aligned with KYC requirements, must be followed and completed for each new account.

8.2.3 The Compliance Officer must periodically reconcile the total number of accounts opened and client codes with corresponding account opening forms and checklists.

8.2.4 Adequate documentation must be collected and maintained regarding the intended nature and purpose of the account to be opened or maintained.

8.2.5 The account opening team should take reasonable measures to verify the accuracy of the information provided by customers during account initiation.

8.2.6 Any updates to a client's profile must be supported by valid documentation and securely maintained by the Account Opening Department.

8.2.7 Departmental Heads must organize regular orientation and training programs to ensure adherence to all relevant laws and AML/CFT obligations.

8.2.8 Customers must receive a Risk Disclosure Document (RDD), in line with the specimen provided by the exchange, outlining the inherent risks of trading in securities.

8.2.9 A written acknowledgment must be obtained from the customer confirming their understanding of the Risk Disclosure Document.

8.2.10 The customer must receive a CDC setup report for signature, along with a complete copy of the Account Opening Form for their records.

8.2.11 The Compliance Department must ensure full adherence to policies and procedures concerning the identification and reporting of suspicious transactions and accounts in line with KYC guidelines.

8.3 Customer Reporting Obligations

8.3.1 The Compliance Function must verify that customer reporting processes comply with regulatory standards, including CDC requirements for balance statements and PSX mandates for account statements.

8.3.2 The Compliance Officer is responsible for ensuring proper documentation of report dispatch and adherence to the customer reporting framework.

8.4 Account Closure Procedures

8.4.1 Account Opening Department must keep comprehensive records of all closed accounts throughout the year and verify closure procedures align with regulatory standards.

8.4.2 The Compliance Department must ensure:

- No outstanding funds or securities remain in customer accounts,
- All funds have been settled and transferred,
- No further transactions have occurred post closure date.

8.4.3 A formal policy must exist for closing accounts, including:

- Settling remaining balances in designated client bank accounts,
- Clear criteria for closure date (i.e., settlement date or account closure request date). Compliance with these guidelines must be confirmed by the compliance function.

8.5 Controls Over Order Placement and Execution

8.5.1 No trades or transactions should be executed by dealers, traders, KATS operators, or any other personnel without explicit instructions from the customer.

8.5.2 The Compliance Department must verify compliance through periodic checks, including the review of trade instructions and matching records.

8.5.3 Authorized personnel must ensure timely and best-effort execution of client orders based on prevailing market conditions.

8.5.4 All telephone-based orders must be recorded using dedicated lines by designated IT staff.

8.5.5 Orders placed in person must be properly documented, and customers must provide acknowledgments. Priority should be given to existing pending orders.

8.5.6 A chronological electronic register of orders, including system logs and telephone recordings, must be maintained.

8.5.7 All written orders—whether by document, fax, email, or other means—must be securely archived.

9. Core Financial Transactions Control

9.1 **Account Operations:** The opening of any bank account and designation of authorized signatories must be approved by the Board. The Finance Department is responsible for fulfilling procedural requirements under the CFO's supervision and must obtain prior board approval for account closures.

9.2 **Bank Reconciliation:** Monthly bank reconciliations must be prepared by the Finance Department and reviewed/approved by the CFO. Any anomalies must be promptly investigated.

9.3 **Fund Disbursement and Receipts:** Finance staff must prepare payment vouchers upon receiving bills/invoices. No payment is processed without authorized approval. All transactions must be properly recorded, and receipts/payments from clients should only be via crossed cheques. Cash transactions exceeding Rs. 25,000 must be reported to the stock exchange.

9.4 **Petty Cash:** The CFO authorizes petty cash use for daily operations. Periodic physical verification must be conducted in the CFO's presence. No petty cash is disbursed without proper documentation and departmental head approval.

9.5 **Profit Computation:** The Finance Department must calculate profits on savings or PLS accounts at applicable rates approved by the CFO. Once credited by the bank, a receipt voucher must be prepared and logged in the system. Any discrepancies require CFO approval.

9.6 **Expense Management:** All expenses exceeding the defined threshold must be pre-approved via purchase orders. All invoices are verified against approved POs. Reimbursement expenses for employees must be properly documented and approved.

10. Information Technology General Controls (ITGC)

10.1 **Access Security:** Access privileges for new or modified users must follow approved protocols. Privileged access is limited and monitored. Password security parameters, such as complexity and expiration, are enforced.

10.2 **Network Operations:** The IT Department must enforce physical and digital safeguards. Daily data backups must be performed, stored securely, and tested regularly to ensure data integrity.

10.3 **System Maintenance:** Guidelines for acquiring, maintaining, and modifying systems/software must be documented and approved by management.

10.4 **IT Governance:** A strategic IT plan is maintained under an IT Committee. A disaster recovery plan is in place, tested regularly, and aligned with the organization's risk management strategy. IT policies are documented, approved, and updated periodically.

10.5 **Network Security:** Unique user credentials, strong password policies, and periodic vulnerability scans are required. Firewalls and intrusion detection systems must be monitored for any threats.

10.6 **Disaster Recovery:** A Business Continuity and Disaster Recovery Plan, approved by the Board, outlines recovery strategies and is tested regularly.

11. Compliance Function

11.1 **Compliance Structure:** A designated Compliance Officer meeting regulatory qualifications is appointed with Board/Audit Committee approval. The officer reports findings directly to the Board/Audit Committee.

11.2 **Board Responsibilities:** The Board, under its Chairperson, ensures internal control systems are in place, oversees operations, and validates the integrity of financial statements.

11.3 **Audit Committee:** A sub-committee of the Board, the Audit Committee assesses internal control effectiveness, reviews audit reports, monitors major risk areas, and validates financial accuracy. It coordinates audits, investigates fraud, reviews related-party transactions, and recommends external auditor appointments.

12. Management and Staff Duties

Management is responsible for daily operations, implementing controls, ensuring compliance, and maintaining efficiency. Responsibilities include:

- Developing policies and monitoring operations,
- Managing risk exposures prudently,
- Ensuring effective internal control systems,
- Safeguarding assets and monitoring business performance,
- Addressing auditor recommendations,
- Complying with regulations and ethics standards,
- Providing annual assurance on internal control effectiveness to the Board.

13. Limitations of Internal Control

While robust internal controls enhance operational reliability and asset security, certain limitations persist:

- Human error due to stress, lack of training, or poor judgment,
- Non-routine transactions escaping standard controls,
- Collusion among staff to override controls,
- Decisions to forego costly controls,
- Delays in updating controls due to process or technology changes.

APPROVED BY

CHIEF EXECUTIVE OFFICER