Persistent

Fraud Risk Management Policy

January 2026

Preamble

Persistent Group ("Company") is committed to maintaining the highest standards of ethics, transparency, and good governance. Fraud and misconduct pose serious risks, eroding trust, disrupting operations, and exposing the Company to financial, legal, regulatory, and reputational consequences. Fraud may be financial (e.g., misappropriation of funds, false invoicing, bribery) or non-financial (e.g., falsification of records, misuse of confidential information, abuse of authority).

The Company upholds a strict zero-tolerance approach toward fraud, corruption, and any form of misconduct, ensuring prompt investigation and decisive disciplinary or legal action, including termination, recovery of losses, and referral to authorities, while fostering a culture of integrity, transparency, and accountability.

To safeguard its brand, reputation, and assets, the Company has established this Fraud Risk Management (FRM) Policy ("Policy"). The FRM framework is guided by global standards, including ISO 37003:2025 and the COSO-ACFE Fraud Risk Management Guide, and incorporates recognized industry best practices to prevent, detect, monitor, and mitigate fraud risks through robust governance, effective internal controls, and continuous improvement measures.

Purpose

The purpose of this Policy is to establish a structured and consistent framework for identifying, assessing, preventing, detecting, and responding to fraud risks across the Company. It outlines the foundational requirements for fraud risk management and provides direction for the development and implementation of effective internal controls. These controls are intended to minimize the risk of fraud, ensure timely detection of irregularities, and facilitate appropriate investigative and corrective actions.

Statutory Requirements (In addition to requirements applicable under the provisions of the Bharatiya Nyaya Sanhita and any other equivalent applicable land law)

1. **Penalties for fraud under Companies Act, 2013:**
   a. **For Fraud involving an amount of INR 10 Lakh in India or USD 10,000 in the US or an equivalent of USD 10,000 in other regions (ROW) or above or 1% of the company's turnover (whichever is lower):**

      - Imprisonment: 6 months to 10 years (minimum 3 years if public interest involved), and
      - Fine: Equal to the amount involved in fraud (may extend to 3 times the fraud amount).

   b. **For fraud involving an amount of less than INR 10 Lakh in India or USD 10,000 in the US or an equivalent of USD 10,000 in other regions (ROW) or 1% of turnover (whichever is lower) and not involving public interest:**

      - Imprisonment: up to 5 years, or
      - Fine: up to INR Fifty Lakh in India or USD 50,000 in the US or an equivalent of USD 50,000 in other regions (ROW), or both.

   c. **Other Penalties:**

      - **Section 448:** Knowingly making a false statement or omitting a material fact in any document required under the Act is punishable with imprisonment and/or fine as per Section 447.

- **Section 449:** Intentionally giving false evidence during examinations or in affidavits related to company matters is punishable with 3-7 year imprisonment and a fine up to INR Ten lakh in India or USD 10,000 in the US or an equivalent of USD 10,000 in other regions (ROW).

2. **Auditor's Reporting Obligations [Section 143(12) & Rule 13 of the Companies (Audit and Auditors) Rules, 2014]:**
   a. **For fraud involving amount INR One Crore in India or USD 110,000 in the US or an equivalent of USD 110,000 in other regions (ROW) or more**, the statutory auditor must:

      - Inform Board or Audit Committee within two days from the date of knowledge of the fraud and seek their response within 45 days;
      - Upon receiving the response, forward the auditor's report along with Board/ Audit Committee's response to the Central Government within 15 days of receipt;
      - If no response is received within 45 days, forward the report to the Central Government along with a note stating that no response was received; and
      - Submit the report electronically via e-Form ADT-4.

   b. **For fraud involving less than the amount of INR One Crore in India or USD 110,000 in the US or an equivalent of USD 110,000 in other regions (ROW)**, the statutory auditor must:

      - Report the matter to Board or Audit Committee within two days, specifying the Nature of Fraud with description, Approximate amount involved; and Parties involved.
      - If reported by the auditors, the Company must disclose such frauds in its Board's Report.

   c. **Fraud Reporting by Other Auditors:**

      - Cost Auditors and Secretarial Auditors must report any fraud detected during their duties in the same manner prescribed for statutory auditors under the Companies Act, 2013.

3. **Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (SEBI LODR) Regulations, 2015:**

   - Fraud or defaults by a listed entity, its promoter, director, key managerial personnel, senior management or subsidiary or arrest of such persons (in India or abroad) must be reported to the stock exchange irrespective of materiality.
   - Frauds or defaults by employees that impact the listed entity materially must also be reported to stock exchange.

Note:

- *Each operating country may have mandatory legal requirements that must be complied with in addition to the Global Policy.*
- *These regional or local requirements will take precedence over the Global Policy in the event of a conflict.*
- *Where both applicable laws and the Global Policy contain similar provisions, the stricter requirement shall prevail.*

Scope

Informed by ISO 37003:2025 guidelines and other industry best practices, this Policy addresses all forms of fraud and misconduct that may impact the Company. It encompasses, but is not limited to:

- Internal fraud against the organization;
- External fraud against the organization;

- Internal fraud in collaboration with business partners or other third parties;
- External fraud in collaboration with the organization's personnel; and
- Fraud by the organization or individuals purporting to act on its behalf or in its interest

This Policy is applicable to all employees, consultants, interns, subcontractors, personnel, subsidiaries, and third-party partners engaged with/by the Company.

Objectives

- Prevent, detect, and respond to fraudulent activities that may impact the Company's interests, assets, operations, employees, stakeholders, and brand reputation;
- Establish clear roles, responsibilities, and accountabilities for fraud risk governance across all levels of the organization;
- Promote ethical conduct, appropriate and consistent organizational behavior through defined guidelines and expectations;
- Align the fraud risk management framework with the Company's strategic goals, ethical standards, and applicable legal and regulatory requirements; and
- Support the development of a proactive fraud risk culture through awareness, training, and continuous improvement initiatives.

Definitions

Fraud refers to any intentional act committed to obtain unlawful or unfair gain, whether in cash or in kind, which causes or could cause social, reputational, or economic harm. Examples include, but are not limited to:

- Deliberate falsification, concealment, destruction, or manipulation of documentation or records intended for normal business purposes
- Misuse of information, authority, or position for personal or financial benefit

Misconduct refers to any act that violates applicable laws, regulations, internal policies, or the Company's Code of Conduct

FRM Governance Structure

The Company's Fraud Risk Management (FRM) governance is structured across four interconnected layers to ensure strategic oversight, effective execution, and operational accountability:

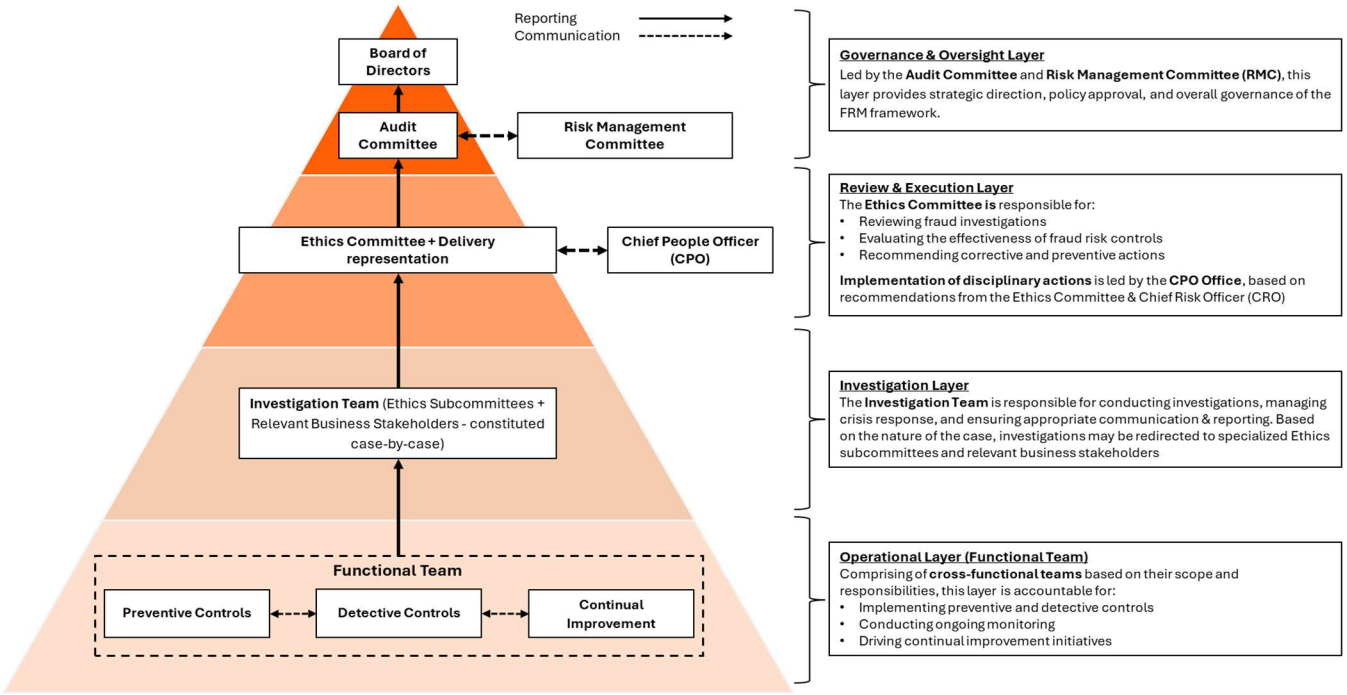

Figure 1: FRM Governance Structure

FRM Framework Overview

To effectively manage fraud risks, the Company implements a comprehensive Fraud Risk Management (FRM) framework embedded within the broader Enterprise Risk Management (ERM) system. This Policy adopts a layered approach combining preventive and detective controls to mitigate fraud risks and ensure timely detection of misconduct. It also defines a structured response mechanism for confirmed or suspected incidents, including investigation, escalation, disciplinary action, reporting, and documentation. The Company is committed to continuous improvement of the FRM framework through periodic evaluation, feedback, and refinement.

This framework is guided by global standards, including ISO 37003:2025 and the COSO-ACFE Fraud Risk Management Guide, as well as other industry best practices, and is built on four foundational pillars.

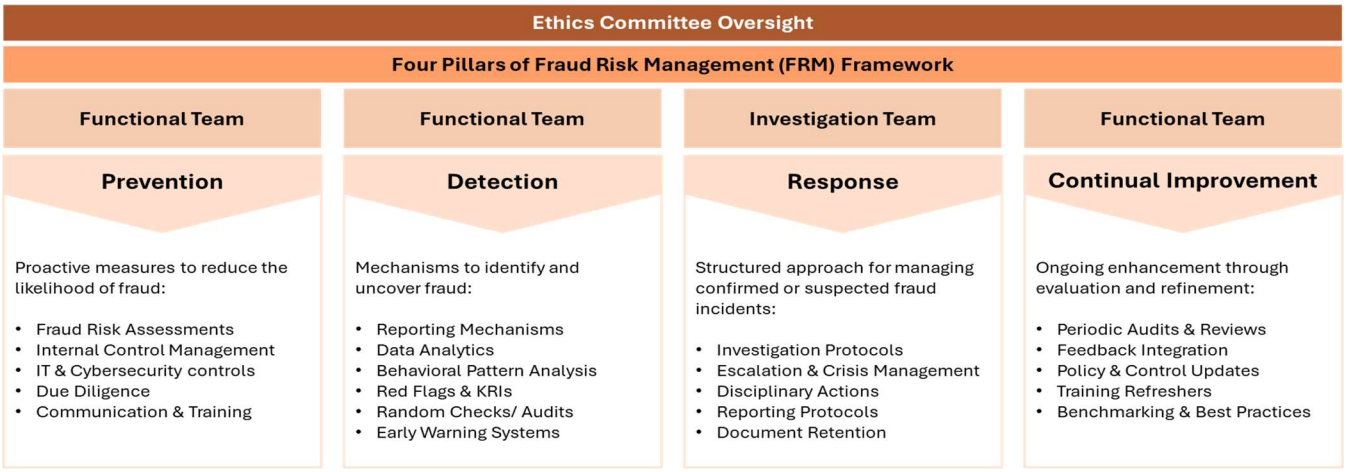

Figure 2: FRM Framework

Reporting Protocols

1. **Internal**:

- Investigation Team submits quarterly case reports to Ethics Committee
- Ethics Committee internally reviews the report on quarterly basis
- Ethics Committee Head to update the Audit Committee / Risk Management Committee (RMC) in quarterly review meetings
- Audit Committee / RMC apprises the Board of Directors as required

2. **External**: Investigation Team collaborates with Corporate Secretarial Team for disclosures under the Companies Act and SEBI LODR regulations (if applicable).

Disciplinary Actions

The Chief People Officer (CPO) Office is responsible for implementing disciplinary actions following investigations conducted by the Ethics Committee. All disciplinary or corrective measures shall comply with applicable laws and adhere to the Company's established procedures.

Relationship with the Code of Conduct and Other Policies:

This Policy complements and operates in conjunction with other Company policies to ensure a cohesive approach to risk governance, ethical conduct, and regulatory compliance. Illustrative related policies include:

- Code of Conduct for Directors and Employees
- Whistle Blower Policy
- Ethics Policy
- Anti-Corruption and Anti-Bribery Policy
- Enterprise Risk Management Policy
- Information Security Policy
- Intellectual Property Rights (IPR) Policy
- Data Governance Policies
- Human Resources Policies
- Administration Policies
- Legal Guidelines
- Significant Accounting Policies
- Responsible AI Policy

Policy Review and Approval Cycle

This Policy shall serve as a guiding document for fraud risk management and will be reviewed at least once every two years, or earlier if there are significant changes in the business environment, regulatory landscape, or organizational structure. Any proposed amendments to the Policy will be reviewed and approved by the Chief Risk Officer (CRO) and Ethics Committee Head as defined in this Policy's governance framework.

Disclaimer

In the event of any inconsistency or conflict between the provisions of this Policy and any applicable law, regulation, rule, or standard, whether existing or newly enacted, the latter shall prevail. The Policy shall be deemed amended to the extent necessary to ensure compliance with such legal or regulatory requirements, until formally revised to reflect the change

****

USA

Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1(408) 216 7010
Fax: +1(408) 451 9177
Email: Info@persistent.com

India

Persistent Systems Limited
Bhageerath,402
Senapati Bapat Road
Pune 411016
Tel: +91(20) 6703 0000
Fax: +91(20) 6703 0008