A simple, practical list to help finance, procurement, and operations teams strengthen fraud prevention processes.

1. People & Responsibilities

☐ Employees receive regular fraud-awareness training

☐ Staff can recognize common fraud schemes (phishing, spoofed invoices, fake vendors)

☐ Employees know how and where to report suspicious activity

☐ Speaking up early is encouraged and supported

☐ Access rights are reviewed at least annually

2. Segregation of Duties (SoD)

☐ No single person can create a vendor, approve invoices, and make payments

☐ Invoice approvals have clear limits based on roles

☐ Payment authorization and invoice approval are separated

☐ System logs are reviewed regularly for unusual actions

☐ Temporary access rights are monitored and removed quickly

3. Vendor Management & Onboarding

☐ All vendors are verified before the first payment

☐ Bank account details are validated and stored securely

☐ Changes in vendor data require independent approval

☐ New or unknown vendors are automatically highlighted

☐ Vendor master data is reviewed and cleaned regularly

4. Invoice Handling & Approvals

☐ Invoices go through a standardized approval workflow

☐ High-value invoices require additional or managerial approval

☐ Duplicate invoice detection is enabled

☐ Audit trails track every approval, change, and comment

5. Purchase Orders (PO) & Matching

☐ POs are created before goods or services are ordered

☐ PO, delivery note, and invoice are matched (3-way match)

☐ Price or quantity discrepancies are flagged automatically

☐ Partial deliveries are controlled and documented

☐ Non-PO invoices follow a strict approval workflow

6. Technology & Alerts

☐ Alerts for new vendors, bank account changes, and unusual activity

☐ e-invoicing is preferred over PDFs for security and traceability

☐ Automated approval workflows reduce human error

☐ Fraud detection rules are updated regularly

☐ Telema eFlow / MatchFlow are fully configured and used consistently

7. Culture & Continuous Improvement

☐ Fraud controls are reviewed at least once per year

☐ Lessons learned are shared across teams

☐ Fraud prevention is discussed openly, without stigma

☐ Employees understand that fraud affects both businesses and private lives

☐ Management communicates clear expectations around fraud resilience