GOLD BRICK GOLD TRADING LLC

AML / CFT / CPF & Targeted Financial Sanctions Compliance HANDBOOK

Version: 1.1 — Effective date: 01-02-2026

Owner: MLRO | Next review: 12 months / regulatory change

Note: This handbook is internal guidance. It does not replace legal advice. Always consult the latest UAE laws, EOCN/CBUAE notices and the UAE FIU (goAML) requirements.

Company: Gold Brick Gold Trading LLC

Jurisdiction: United Arab Emirates

Policy Owner: Money Laundering Reporting Officer (MLRO)

Review Cycle: Annual

Applicability: All staff, management, directors, contractors

TABLE OF CONTENTS

1. PURPOSE & SCOPE

Purpose

This handbook establishes a comprehensive AML/CFT/TFS/CPF framework for **Gold Brick Gold Trading LLC (GBGT)** to:

- Prevent, detect, and report money laundering, terrorist financing, counter-proliferation financing, and breaches of targeted financial sanctions arising from gold trading activities.
- Align with **UAE Federal Decree-Law No. 20 of 2018**, **Cabinet Decision No. 10 of 2019**, **Cabinet Decision No. 74 of 2020**, **FATF** standards, **UN** sanctions regimes, **EOCN** directives, **MoE DNFBP** rules, **CBUAE** guidance, and **OECD Responsible Gold Supply Chain** guidance.
- CPF (Counter-Proliferation Financing) obligations are addressed in accordance with Cabinet Decision No. 74 of 2020 and EOCN directives
- Establish clear procedures for customer, supplier, and transaction risk management
- Protect the reputation, licenses, and assets of **Gold Brick Gold Trading LLC** ("GBGT")

Scope

This policy applies to:

- All employees, directors, shareholders, agents, and contractors
- All business activities including purchase, sale, import/export, storage, logistics, and financing of gold
- All customers, suppliers, intermediaries, transporters, refiners, and financial counterparties

DNFBP Classification

Gold Brick Gold Trading LLC is classified as a **Designated Non-Financial Business or Profession (DNFBP)** under UAE law, operating as a **Dealer in Precious Metals and Precious Stones (DPMS)**.

Accordingly, GBGT applies AML/CFT/CPF/TFS obligations to:

- All business relationships; and
- Occasional or one-off transactions involving cash or interrelated transactions of **AED 55,000 or more**, in line with MoE DNFBP requirements.

2. REGULATORY & LEGAL FRAMEWORK

GBGT complies with

UAE Laws & Regulations

- Federal Decree-Law No. (20) of 2018 – AML/CFT
- Cabinet Decision No. (10) of 2019 – Implementing Regulations
- Cabinet Decision No. (74) of 2020 – Targeted Financial Sanctions
- Ministry of Economy (MoE) – DNFBP Guidelines
- UAE Financial Intelligence Unit (FIU) – goAML obligations

Sanctions & Non-Proliferation

- United Nations Security Council Resolutions
- UAE Local Terrorist List
- Executive Office for Control & Non-Proliferation (EOCN)

International Standards

- FATF Recommendations
- OECD Due Diligence Guidance for Responsible Supply Chains of Gold

3. GOVERNANCE, OVERSIGHT & ROLES

Board of Directors

- Approves AML/CFT policy and risk appetite
- Ensures adequate resources and independence of Compliance
- Reviews EWRA and compliance reports

Senior Management

- Implements policy, assigns budgets/people/technology; resolves escalations; signs off on high-risk relationships.
- Approves high-risk relationships
- Ensures remediation of audit findings

Money Laundering Reporting Officer (MLRO)

- Owns AML/CFT/TFS/CPF program; maintains EWRA; approves onboarding as per authority matrix.
- Reviews ISRs and files STRs via goAML
- Handles sanctions TFS freezing and EOCN reporting
- Liaises with FIU, MoE, CBUAE, and EOCN
- Maintains confidential registers
- The MLRO has direct and unrestricted access to Senior Management and the Board and operates independently of business lines

Compliance Team

- Conducts KYC, CDD, EDD, screening, and monitoring
- Maintains records and risk assessments

- Performs quality assurance and testing

Front Office / Trading / Procurement

- Collect KYC and supplier documentation; perform first-line checks; immediately file ISRs on suspicion.

Operations / Warehouse / Logistics

- Validate chain-of-custody; check transport documents; perform inspections; hold goods on compliance instruction.

Finance / Payments

- Verify payment instructions; reject unrelated third-party payments; assist STR evidence pack.

Internal Audit / Independent Reviewer

- Annual independent review of design & operational effectiveness; track remediation.

All Staff

- Complete training; adhere to procedures; never “tip-off”; report concerns via ISR.

4. ENTERPRISE-WIDE RISK ASSESSMENT (EWRA)

Objectives

- Identify and evaluate inherent ML/TF/CPF/TFS risks; assess control strength; determine residual risk and risk appetite alignment.

Methodology

- Factors & indicative weights (calibrate to business):
  - Customer (type, cash-intensity, UBO opacity, PEP ties) — 25%
  - Geography (origin, transit, destination, sanctions/weak AML regimes) — 25%
  - Product/Service (bullion vs scrap; hand-carry; third-party payments) — 20%
  - Delivery Channel (non-face-to-face, introducers) — 10%
  - Sanctions/CPF Exposure (list proximity, dual-use risk) — 20%

Scoring

- 1–5 scale per factor; sum to total score. Example thresholds (illustrative): Low / Medium / High — calibrated and documented in the formal EWRA.

Frequency & Triggers

- Annual formal EWRA; event-driven updates for market/route/product changes, sanctions updates, adverse media, audit findings.

Outputs & Documentation

- Company Risk Register; mitigating controls matrix; Board approval minutes; evidence retained ≥ 5 years.

5. CUSTOMER ONBOARDING PROCEDURE (step-by-step, operational)

1. Pre-screening (immediate)

- Name search vs UN Consolidated List, UAE Local Terrorist List, internal watchlist, PEP database, and adverse media sources.

  If match -> pause & escalate.

2. KYC Document Collection

- **Individual**: Passport, Emirates ID/National ID (copy), proof of address (utility/bank statement last 3 months), photo/selfie for biometric match, occupation.
- **Corporate**: Trade license, Certificate of Incorporation, Memorandum & Articles, shareholder register, BO Declaration, board resolution authorising signatory.

3. Verification

- Verify documents via government registries or certified third-party providers. For non-face-to-face: use robust electronic identity verification and video call with liveness detection where available

4. Beneficial Ownership

- Identify UBOs holding ≥ 25% or natural persons exerting control. Trace through nominee/shareholding chains.

5. Risk Assessment & Scoring

- Populate risk matrix and score. Determine CDD or EDD.

6. Sanctions/PEP/Adverse Media

- Document outcome, attach screenshots, save search logs.

7. Approve / Reject / Defer

- Low/Medium risk: delegated Compliance sign-off.
- High risk: MLRO + Senior Management or Board.

8. System Entry & Ongoing Monitoring

- Enter customer into compliance system, set periodic review reminders (Low 36 months / Medium 24 months / High 12 months or more frequently).

9. Onboarding Checklist (must be complete before first trade)

- KYC documents obtained & verified; BO identified; sanctions/PEP checks; risk score & approval; payment instructions verified.

6. CUSTOMER DUE DILIGENCE (CDD) – FULL CHECKLIST

Minimum CDD (Individuals)

- Full legal name, date of birth, nationality.
- Valid ID/passport; Emirates ID / National ID where relevant.
- Address proof (utility, bank statement).
- Contact details.
- Occupation/employer; expected transaction profile; declaration of source of funds.

Minimum CDD (Legal Entities)

- Legal name & registration; trade license; certificate of incorporation.
- MOA/AOA; list of directors & authorized signatories.
- UBO details (≥25%); verification for each UBO.
- Beneficial ownership includes natural persons who ultimately own or **exercise control through other means**, including voting rights, veto rights, shareholder agreements, or senior management control, even where ownership is below 25%.
- Ownership chain charts are mandatory for entities with two or more layers.
- Nature of business; expected turnover and transaction profile.
- Bank references where available.

Verification standards

- Use authenticated copies or official registries; do not accept expired IDs as sole proof.

Sanctions & PEP screening

- Required pre-onboarding and prior to every transaction for medium/high risk or as configured: UN, UAE, EOCN lists, and commercial lists where available.

Ongoing monitoring

- Transactions to be monitored for conformity with expected profile; investigate material deviations.

CDD documentation retention

- Store KYC and copies of verification evidence for minimum 5 years after relationship termination.
- CDD shall also be conducted for occasional or one-off transactions, including interrelated transactions, meeting or exceeding AED 55,000, or where suspicion exists regardless of amount

7. SUPPLIER DUE DILIGENCE (OECD-ALIGNED)

Purpose

- Prevent intake of conflict, illicit, or sanction-tainted gold and ensure responsible sourcing.

OECD Five-Step Implementation (applied)

1. Management systems
    - Board-approved Responsible Sourcing Policy.
    - Supplier Code of Conduct (human rights, anti-corruption, environmental).
    - Written contracts with audit and termination clauses.
    - Grievance/whistleblowing mechanism.
2. Identify & assess risks
    - Map full supply chain: mine → trader → refiner → transporter → seller.
    - Country-level risk: conflict areas, weak governance, corruption indices.
    - Supplier-level: shell companies, lack of premises, cash-for-gold practices.
3. Design & implement response
    - Ask for documents: origin declarations, assay certificates, export permits, customs declarations, invoices, BL/airway bills, chain-of-custody records, refinery certificates.
    - For medium/high risk: require corrective action plan, temporary suspension, or reject.
4. Independent third-party audit
    - Annual audits for high-risk suppliers or ad-hoc audits after major red flags.

    - Use accredited audit firms with minerals supply chain experience.

5. Reporting
    - Annual Responsible Sourcing Report summarizing due diligence, audits, incidents, remediation.

Operational Supplier Checklist

- Company registration & licenses.
- UBO and director verification.
- Chain-of-custody documents (mine of origin; refiner assay certificates).
- Transport routes & carrier verification.
- Payment terms and whether cash is used.
- Sanctions/PEP/adverse media checks.
- ESG policy & grievance process.

Contract clauses (recommended)

- Warranties of lawful origin.
- Right to audit & inspect.
- Immediate termination for confirmed conflict/gross violations.
- Indemnity for misrepresentation.

On-site inspections

- Inspect warehouse, weigh scales, sample chain, segregation processes.
- Verify staff lists, invoices, suppliers, and packing lists.

Recordkeeping

- Supplier due diligence file; retain for 5+ years.

8.ENHANCED DUE DILIGENCE (EDD)

When to trigger EDD

- Customer is a PEP or associated to a PEP.
- Customer is from FATF high-risk/greylist country or subject to sanctions scrutiny.
- Large or unusual cash transactions (cash thresholds e.g., AED 55,000 and above — company should treat single/linked amounts hitting that figure as subject to enhanced due diligence and internal escalation per UAE guidance).
- Complex ownership (offshore trusts, bearer shares, nominee arrangements).
- Adverse media indicating criminality or serious reputational risk.

EDD Steps (operational)

1. Senior Management approval: No onboarding without written approval.
2. Documentary evidence of Source of Funds (SOF): Invoices, bank statements (last 12 months), sale/purchase contracts.
3. Source of Wealth (SOW): Audited financials, tax returns, sale of assets docs, corporate minutes.
4. Independent checks: Additional public records, registry checks, bank confirmation.
5. Site verification: On-site inspection, supplier factory/office visit or third-party verification service.
6. Transaction restrictions: Set lower limits and require pre-approval for each trade.
7. Monitoring: Move to monthly or real-time transaction monitoring.

8. Document decision & rationale: Save approvals, evidence, and ongoing monitoring plan.

Periodic EDD Review

- For ongoing relations, EDD revalidation at least every 6–12 months or sooner upon adverse development.

9. PEP & ADVERSE MEDIA SCREENING (EXPANDED)

PEP definition & scope (operational)

- Domestic PEPs: Senior UAE officials, senior military/police/judicial, senior SOE execs.
- Foreign PEPs: Equivalent positions abroad.
- International organization PEPs: Senior staff in organizations like UN, IMF, World Bank.
- RCAs: Immediate family (spouse, parents, children, siblings) & known close associates/business partners.

Screening tools & coverage

- Licensed global PEP databases (e.g., World-Check, Dow Jones, LexisNexis) and local registers.
- Cross-check typographical variants, prior names, transliterations, aliases.
- Capture corporate links (director appointments, board memberships).

Frequency & cadence

- **At onboarding**: mandatory.

- **Ongoing**: daily automated screening for active clients; manual quarterly validation for all high/medium risk clients; immediate re-screen on trigger events (news, sanctions update).

Handling PEP matches

1. **Potential match**: pause onboarding/transactions; collect identifying info (DOB, ID).
2. **Confirm match**: treat as PEP — automatic High risk; EDD applies.
3. **Senior approval**: MLRO + Senior Management sign-off required to proceed with relationship including conditions (limits, monitoring).
4. **Monitoring**: set monthly transaction review; lower thresholds for alerts.

Adverse Media screening — procedure

- Sources: global/regional newspapers, regulator releases, court records, NGO reports, official notices.
- Multi-lingual coverage: include primary languages relevant to customer operations.
- Assessment of relevance: ensure it refers to the same person/entity (cross-reference DOB, location, business).
- Severity classification:
    - **High**: Corruption, money laundering, terrorism links, sanctions, CPF indicators → likely decline or EDD + remediation + senior review.
    - **Medium**: Regulatory fines, fraud allegations → EDD + mitigation.
    - **Low**: Minor civil matters → note & monitor.

Documentation & evidence

- Save media clipping, URL, screenshot, date/time, analyst name, decision memo. All stored in KYC file.

Risk Decision Factors:

- Severity of allegation
- Credibility of source (official vs media/blog)
- Recency
- Jurisdictional relevance
- Linkage confidence

Outcomes:

- Decline
- EDD with mitigation
- Accept with enhanced monitoring

10.INTERNAL SUSPICIOUS REPORT (ISR) — staff-facing procedure

Purpose

- Provide secure, fast internal escalation so MLRO can assess and decide on STR.

Who files

- Any staff member who notices unusual customer behaviour, transaction anomalies or red flags.

When to file

- Immediately / same business day once suspicion arises (company policy: within 24 hours).

ISR content (minimum)

- Reporter details (name/department).
- Customer/Supplier name & account ref.
- Transaction(s) date(s), amount(s), currency, channel.
- Why suspicious: red flags checklist ticked and short narrative.
- Supporting documents attached (invoices, SWIFT, BL, emails, screenshots).

Submission channels

- Secure email to MLRO (encrypted) or sealed hand-delivery to Compliance team; flagged as CONFIDENTIAL.

MLRO initial response

- Acknowledge receipt to reporter (no details about escalation).
- Log ISR in confidential ISR register.

- Preliminary triage within 24 hours: request additional info or escalate to investigation.

Confidentiality & protections

- Protect reporter identity; anti-retaliation policy applies.

11.SUSPICIOUS TRANSACTION REPORT (STR) — MLRO process & goAML filing checklist

STR decision criteria

- **"**Reasonable grounds" to suspect involvement in ML/TF/CPF or TFS breach.
- An STR shall be filed without delay once reasonable grounds for suspicion are established.
- Internal escalation timelines (ISR → MLRO) are governed by internal SLAs (within 24 hours).

STR preparation steps

1. Consolidate ISR evidence: KYC, transactions, emails, shipment docs, payment traces.
2. Analytical narrative: Chronological storyline, indicators observed, reasons for suspicion.
3. List of parties: Customer, beneficial owners, counterparties, intermediaries, banks.
4. Transaction trail: Dates, amounts (currency), account numbers, payment routes, instrument types.

5. Attachments: IDs, invoices, assay certificates, BL, SWIFT messages, email chains, screenshots of screening hits.
6. Mitigation steps taken: Holds, freezes, refusals, suspension of shipments, bank contact.

goAML filing

- Submit via goAML portal using company's registered account. Include as much detail as possible; mark confidentiality and reference.

Post-STR actions

- Ongoing monitoring, cooperate with FIU requests, preserve evidence, hold transactions per FIU/EOCN instruction.

Retention & logs

- Keep STR and supporting documents for at least 5 years from filing.

Tipping-off

- Never inform customer or third party of suspicion or STR filing (criminal offence).

Suspicious attempted transactions, including declined, blocked, or abandoned transactions, are subject to ISR, STR, and TFS reporting obligations

12.TARGETED FINANCIAL SANCTIONS (TFS) & COUNTER PROLIFERATION FINANCING (CPF) — procedures

TFS: obligations & coverage

- Screen against UN Consolidated List + UAE Local Terrorist List (EOCN) + other lists deemed relevant.
- Prohibit any dealing with designated persons or entities.

Immediate actions on match (confirmed)

1. Immediate freeze without delay (within 24 hours) of all funds, assets, goods, or economic resources owned or controlled (directly or indirectly) by a designated person/entity.
2. Notification and reporting to EOCN and the relevant Supervisory Authority within two (2) business days, unless otherwise instructed.
3. Freezing obligations apply regardless of ownership percentage if control is established.
4. Isolate: Segregate funds/goods; prevent release.
5. Escalate: Notify MLRO, then EOCN per reporting procedure.
6. Record: Maintain audit trail of freeze action.

Register → Screen → Freeze → Notify

Handling false positives

- Conduct secondary checks (DOB, nationality, alias, UBO chain) and document rationale if unfreezing.

CPF-specific controls (beyond list matching)

- Identify dual-use goods and requests for unusual end-use or end-users.
- Scrutinize trade documents for inconsistencies (freight forwarder mismatch, inconsistent HS codes, mismatched values).
- Ask for end-user certificates; verify authenticity with issuing authority.

Coordination with banks & counterparties

- If counterparties request instructions, coordinate through MLRO and legal counsel; do not release funds until clearance.

Suspicious attempted transactions, including declined, blocked, or abandoned transactions, are subject to ISR, STR, and TFS reporting obligations

13.EOCN COMPLIANCE — operational protocol

Registration & access

- Maintain registered EOCN account; confirm authorized users and contact points.

Daily operations

- Automate list ingestion (UN + EOCN + other lists). Run daily batch and pre-transaction screenings.

Freeze reporting

- Use EOCN prescribed format; include immediate action logs (time stamps, persons involved).

Nil reporting & ongoing engagement

- File nil reports if required by instruction. Keep open communications with EOCN during investigations.

Audit & testing

- Include sanctions controls in annual compliance testing and run false positive rates analysis.

14. CENTRAL BANK OF UAE (CBUAE) GUIDELINES – APPLICATION

GBGT aligns its AML/CFT/CPF/TFS framework with CBUAE expectations as a supervisory benchmark, recognizing that its banking partners are regulated entities.

CBUAE expectations (applied as benchmark)

- **RBA**: document EWRA and apply controls proportionate to risk.
- **CDD & EDD**: UBO verification, source of funds checks for high risk, face-to-face verification where possible.
- **Transaction Monitoring**: generate automated alerts and investigate promptly.
- **Reporting**: timely STR and sanctions reports.
- **Training & Audit**: scheduled training and independent program testing.

Operationalization

- Periodic policy review aligned to CBUAE guidance.
- Maintain logs, evidence of management sign-offs and training attendance.

15. TRANSACTION MONITORING & RED FLAGS (GOLD SPECIFIC)

Monitoring focus

- Value/weight anomalies, frequency, remitters/beneficiaries, payment methods, routing, unusual discounting/premium patterns.

Red Flags (extensive)

- High-value cash purchases inconsistent with customer profile.
- Splitting a large transaction into multiple smaller transactions (structuring).
- Multiple transactions with different counterparties but common UBO.
- Third-party or unrelated payments for gold purchases.
- Rapid resale of gold in different jurisdiction with unusual margin.
- Inconsistent or falsified assay/certificate details.
- No logical commercial rationale for routing/transshipment.
- Refusal to provide supplier/origin documentation.

- Frequent changes of shipping instructions or last-minute rerouting.
- Use of shell companies and nominee directors, especially with opaque jurisdictions.
- Payment to or receipt from banks in jurisdictions under heavy sanctions or with weak controls.

Investigation steps on alert

- Gather supporting documents; compare to expected profile; interview front-office; file ISR if unresolved.

Trade-Based ML Controls (Gold-Specific):

- Spot price vs invoice price reasonableness checks
- Weight, purity, assay vs invoice reconciliation
- Shipment route logic review
- Split shipment / split payment detection
- Third-party payment prohibition (exceptions only with MLRO approval)
- Buy-back or circular trading detection

16. RECORDKEEPING, RETENTION & DATA PROTECTION

What to keep

- Full KYC/CDD files, UBO documentation, EDD evidence, supplier DD files, transaction records, screening logs, ISR/STR filings, sanctions freeze logs.

Retention period

- Minimum 5 years from relationship termination or date of transaction. Some matters (FIU investigations) may require longer retention — retain until notified.

Security & access

- Use encrypted storage / role-based access; audit trails for access to records. Comply with UAE data protection requirements.

All AML/CFT/CPF/TFS records must be retrievable within 48 hours upon request by regulators or competent authorities

17. TRAINING & INDEPENDENT REVIEW

Training program

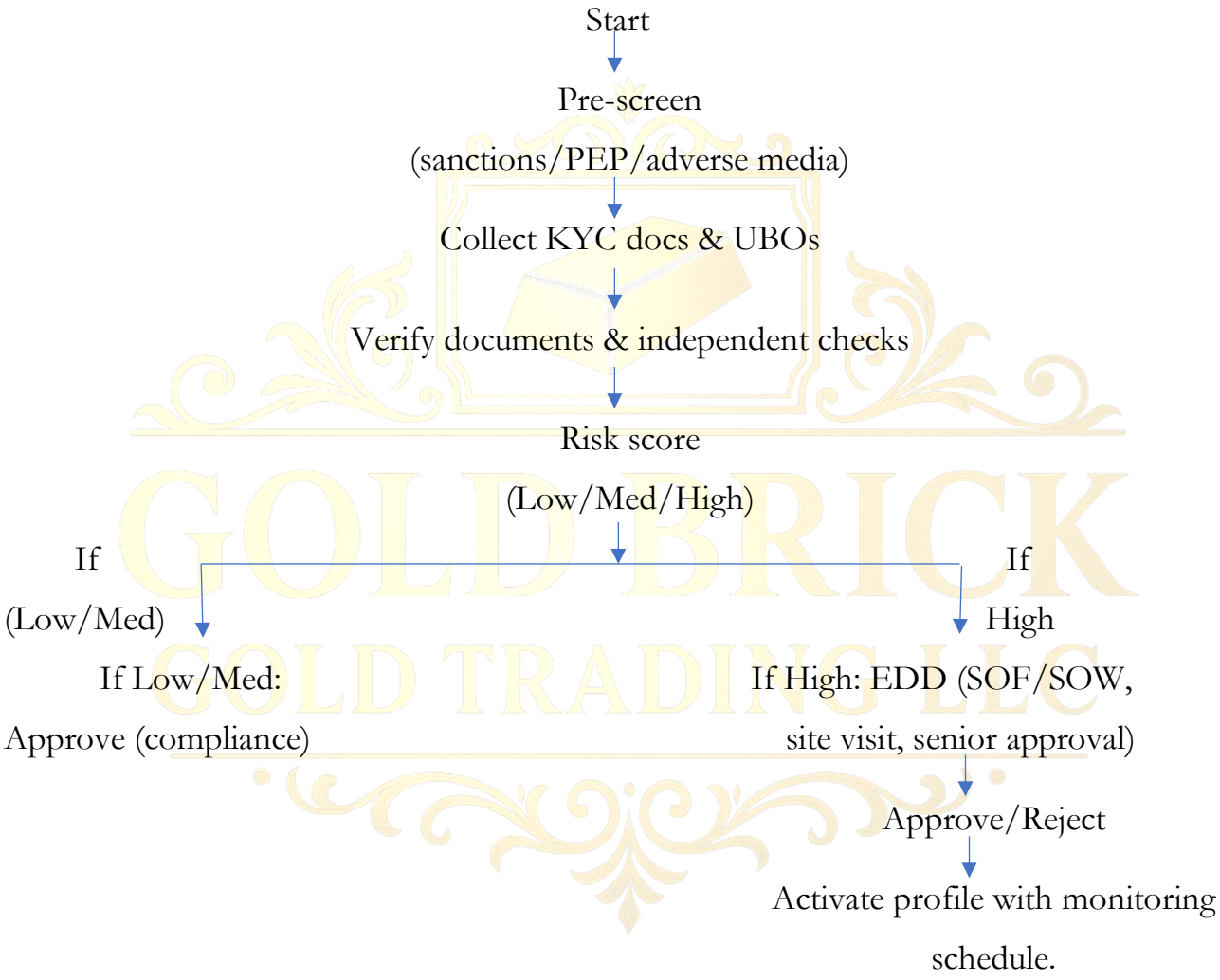
- **Induction**: AML/CFT basics for all new hires within first 30 days.
- **Annual refresher**: Mandatory for all staff.
- **Role-based**: Additional modules for front-office, procurement, finance, logistics, compliance.
- **Scenario-based**: ISR drafting, sanctions freeze exercises, CPF scenarios.

Testing & assurance

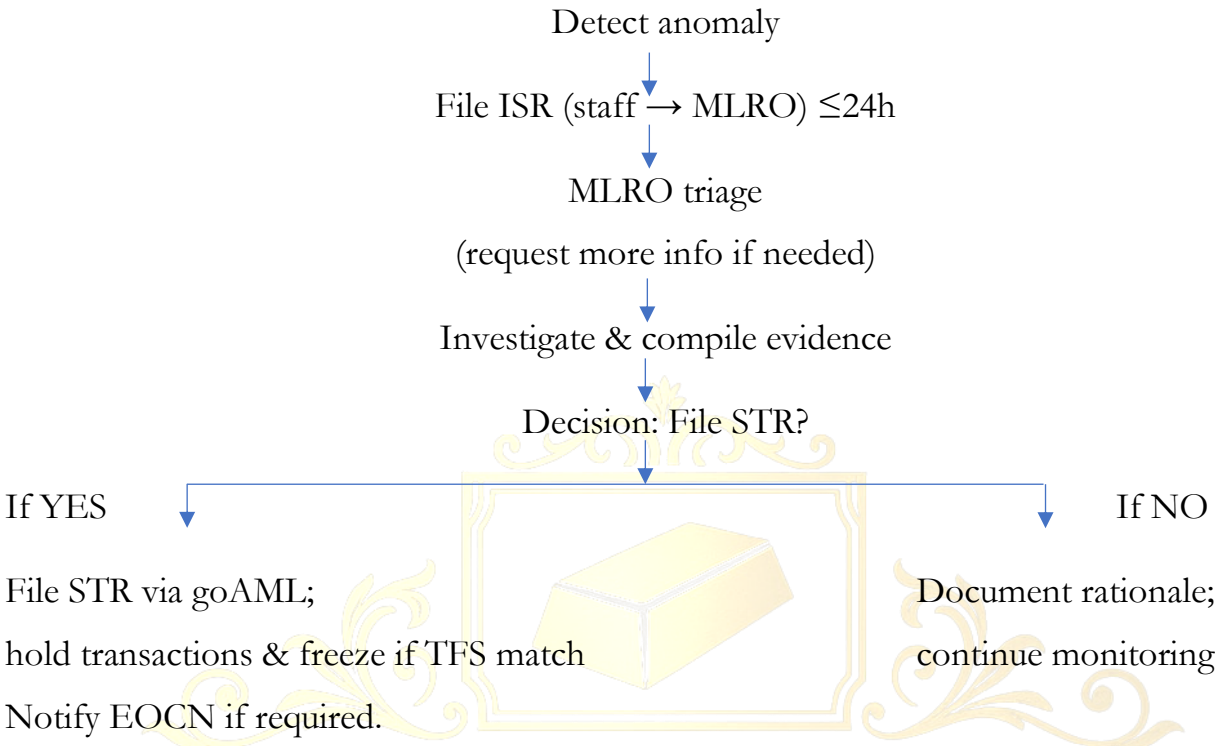
- Quarterly compliance monitoring checks.
- Annual external independent audit covering design and operating effectiveness of controls.
- Remediate findings and track corrective actions.

18. FLOWCHARTS (VERTICAL TEXT VERSION)

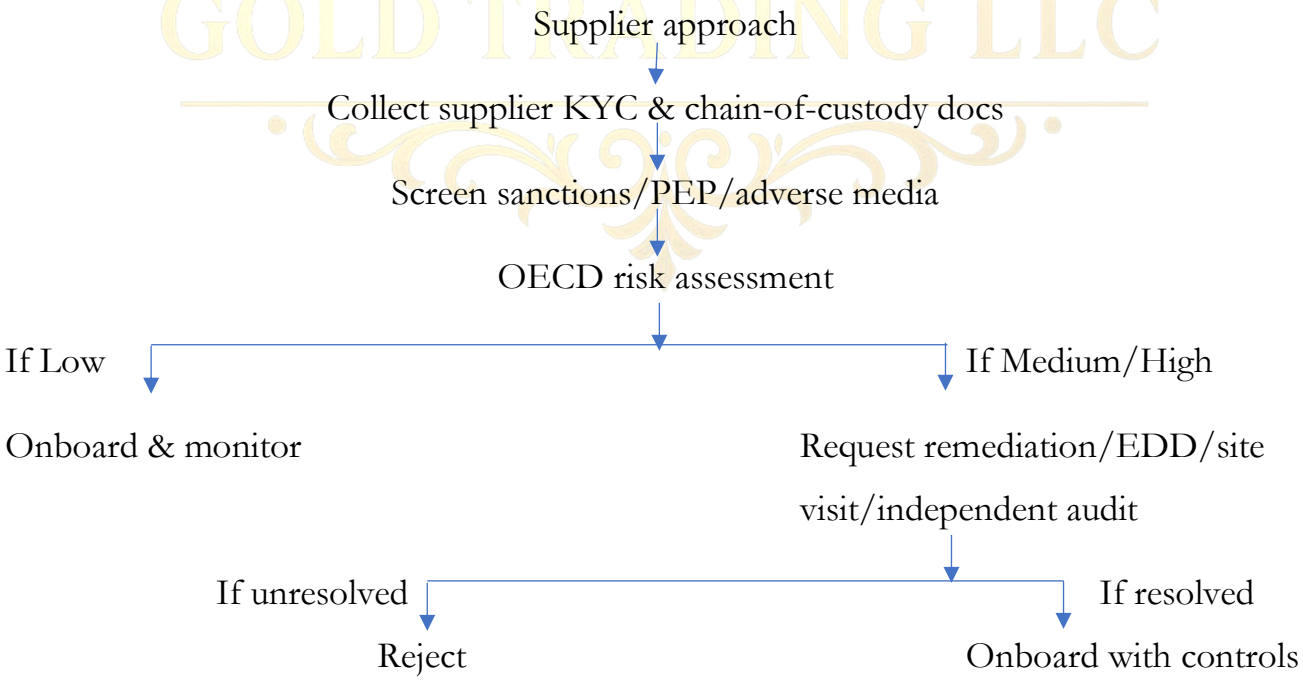
A. CDD / Onboarding



B. ISR → STR



C. Supplier Due Diligence



19. TEMPLATES & FORMS (FIELD LISTS)

19.1 Customer KYC Form (fields)

- Customer type (ind / corp) / Legal Name / Trading Name
- Registration / Passport / Emirates ID / DOB / Nationality
- Address / Contact / Email / Phone
- Business description / Expected turnover / Kg/month
- UBO list (Name / ID / % ownership / nationality)
- Source of Funds (summary + docs attached)
- Sanctions / PEP / Adverse Media result (tool, date, analyst)
- Risk Rating & rationale
- Compliance sign-off (name, date)

19.2 ISR Form (fields)

- Reporter name / dept / date/time
- Customer / Supplier / Account / TXN ID
- Amount / currency / instrument / payment route
- Narrative: what, why suspicious (tick red flags)
- Documents attached (list)
- MLRO acknowledgement (date/time)

19.3 STR Checklist (for MLRO)

- Attach KYC/UBO evidence, ISR, transaction trail, shipping docs, payments, emails, phone logs, assay certs. Provide succinct narrative and requested FIU keywords.

19.4 Supplier DD Questionnaire (excerpt)

- Legal name / reg number / license / tax id
- UBO(s) and directors list
- Mine/refinery origin / assay certificates / export permits
- Transport route & carrier details
- Payment terms; any cash involvement?
- ESG policy & grievance mechanism?
- Declaration: "Goods supplied are not sourced from conflict-affected or high-risk areas" (signed & dated)

19.5 Record Log templates

- Screening logs; ISR register; STR register; Sanctions freeze log; Audit remediation tracker.

20. EXIT / REFUSE / DE-RISKING POLICY

Grounds to refuse/onboard exit

- Confirmed sanctions or CPF involvement; unresolved adverse media or credible evidence of criminality; failure/refusal to provide UBO/SOF/SOW; unacceptable audit findings from supplier/inability to remediate; persistently high false positive that cannot be resolved.

Procedure on exit

- Stop transactions, freeze as required, notify operations/warehouse to hold shipments, document exit rationale, notify relevant authorities if required. Apply secure data retention.

Where exit or refusal is linked to ML/TF/CPF/TFS suspicion, the MLRO shall assess whether an STR or sanctions report is required prior to or concurrent with exit."

Below is a **FORMAL, REGULATOR-SAFE DISCLAIMER** you can place on the **cover page or final page** of your AML/CFT policy and handbook.
It is written to satisfy **UAE MoE / DMCC / bank audit expectations**, while protecting the company legally.

23. DISCLAIMER

This Anti-Money Laundering, Counter-Terrorist Financing, Counter-Proliferation Financing and Targeted Financial Sanctions Policy ("AML Policy") has been developed by **Gold Brick Gold Trading LLC** ("the Company") for **internal governance and compliance purposes only**.

This AML Policy:

- Is intended to outline the Company's internal controls, procedures, and risk-based framework designed to comply with applicable **UAE AML/CFT/CPF laws**, **Ministry of Economy (MoE) DNFBP guidelines**, **Executive Office for Control & Non-Proliferation (EOCN) directives**, and relevant international standards including **FATF recommendations**.
- Does **not constitute legal, regulatory, financial, or tax advice**, and should not be relied upon as a substitute for professional legal or regulatory guidance.
- Is based on laws, regulations, and regulatory guidance in force at the time of issuance and may require updates to reflect future legislative or regulatory changes.

The Company reserves the right to:

- Amend, update, or replace this AML Policy at any time in response to changes in law, regulation, risk profile, or supervisory expectations.
- Apply enhanced or additional controls beyond those described in this AML Policy where deemed necessary under a risk-based approach.

Nothing in this AML Policy:

- Creates contractual rights or obligations with any third party.
- Limits the Company's discretion to decline, suspend, or terminate any business relationship.

- Restricts the Company's obligation to cooperate with competent authorities, including the **UAE Financial Intelligence Unit (goAML)**, **MoE**, **EOCN**, or other regulators.

In the event of any inconsistency between this AML Policy and applicable UAE laws, regulations, or official guidance, the **applicable laws and regulatory requirements shall prevail**.

21. DOCUMENT CONTROL & SIGN-OFF

22. **Policy Owner: MOSES JAYARAJ**

23. **Approval: MOSES JAYARAJ**

24. **Effective Date: 01/02/2026**

25. **Version History: V 1.1**

26. **Next Review Date: 01/02/2027**

Company Stamp