UDB Logistics

# Supplier Due Diligence (UAE)

APPLIES TO
UDB Logistics FZCO (DIEZ)

GOVERNING LAW
UAE / Dubai Courts

VERSION
v1.0

EFFECTIVE DATE
14 Feb 2026

LAST UPDATED
19 Feb 2026

DOC ID
UDB-UAE-SUPPLIER-DUE-DILIGENCE-v1.0

OWNER
Compliance (Head of Compliance)

CONTACT
compliance@udb.ae

## 1. Purpose

This Supplier Due Diligence framework describes how UDB Logistics FZCO (DIEZ) (“UDB”) screens, approves, and periodically re-assesses suppliers and operational partners to reduce compliance, security, and service risks in connection with logistics services arranged by UDB in the UAE.

## 2. Scope

This framework applies to suppliers and third parties engaged by UDB to support shipment execution and related services, including (as applicable):

- airlines / GSA / carrier-related counterparties;
- ground handlers and terminal operators (e.g., cargo terminals);
- trucking / transport partners;
- warehouses and bonded facilities;
- DG service partners and packing/repacking vendors;
- screening/security service providers;
- customs brokers/agents (where used);
- IT/communications service providers supporting operational processing (where relevant);
- any subcontractor with custody access to cargo, shipment documents, or customer data.

This document is intended for onboarding and risk controls. It does not replace shipment-specific operational decisions or third-party contractual terms.

## 3. Due diligence approach and tiers

UDB applies a tiered due diligence approach based on risk profile, custody exposure, and regulatory sensitivity.

### 3.1 Tier A — Standard

Use when: low-to-moderate risk supplier, established market participant, limited custody exposure, low compliance complexity.

Typical examples: established trucking partner for standard routes, basic service vendors with limited access.

### 3.2 Tier B — Enhanced
Use when: supplier has direct custody access, handles sensitive documentation, operates in higher-risk lanes, or supports regulated workflows (DG/export controls).

Typical examples: warehouse partners, transport partners with custody, DG packing/repacking, customs interface support.

### 3.3 Tier C — Critical (High-Value / High-Risk)
Use when: supplier is involved in high-value shipments, theft-attractive commodities, sensitive routings, security incident history, or strategic goods controls.

Typical examples: high-value warehouse custody, high-risk trucking, regulated/strategic goods workflows, special security chain-of-custody requirements.

Tier assignment is determined by UDB based on custody access, value exposure, compliance risk, routing, and supplier history. UDB may upgrade or downgrade tiers at any time based on new risk information.

## 4. Minimum onboarding pack (supplier information)
Unless not feasible due to market structure (e.g., certain monopoly/authority-operated terminals), UDB requests the following baseline information before approval:

### 4.1 Supplier identification (minimum)
- Legal name and trade name (if different)
- Registration/trade license evidence (UAE or relevant jurisdiction)
- Registered address and operational site(s)
- Authorized signatory / management contact
- VAT status (if applicable in their jurisdiction)
- Bank account details for payments (where relevant)

### 4.2 Operational capability (minimum)
- Description of services provided
- Coverage (locations, routes, operating hours)
- Primary contact(s) for operations and escalation
- Any special capabilities (DG, temperature handling, bonded ops)

### 4.3 Insurance and liability (where applicable)
Where the supplier provides custody/transport/warehouse services, UDB may request evidence of applicable insurance and/or standard liability terms (as available), recognizing that coverage varies by supplier and market practice.

## 5. Compliance screening and checks
UDB performs compliance checks proportionate to the supplier tier and role.

### 5.1 Sanctions and restricted party screening
UDB screens supplier legal name and relevant principals (where available) against:

- UN sanctions lists

- UAE applicable lists and requirements
- and, where commercially required, additional lists (e.g., OFAC / UK / EU), depending on banking, carrier, insurance, or customer requirements.

Potential matches are escalated for manual review. Confirmed matches result in rejection or termination, subject to applicable law.

### 5.2 Export control / strategic goods exposure

Where the supplier supports export control workflows or strategic goods handling, UDB may assess:

- ability to support approvals/clearances;
- operational controls to prevent unauthorized release;
- documentation handling discipline.

### 5.3 Adverse media and integrity flags (risk-based)

For Tier B/C suppliers (and where reasonable), UDB may perform basic adverse media review and consider integrity risk indicators (e.g., fraud, theft allegations, repeated compliance issues).

## 6. Security & quality controls (operational due diligence)

For suppliers with custody access (especially Tier B/C), UDB assesses operational security and quality controls proportionate to risk. This may include:

### 6.1 Cargo security and access discipline

- access control to cargo areas (restricted access / role-based control where feasible);
- visitor and staff controls where applicable;
- measures to reduce dwell time and unauthorized access.

### 6.2 Evidence and chain-of-custody (where applicable)

For Tier C or high-value workflows, UDB may require or prioritize:

- ability to provide handover proof / acceptance record;
- piece count / condition checks at key handover points;
- incident evidence preservation support (e.g., CCTV retention request process).

### 6.3 Incident handling capability

- ability to raise irregularity reports where applicable;
- internal escalation contacts and response expectations;
- cooperation on evidence preservation and factual timelines.

### 6.4 Quality and performance signals

UDB may track and review supplier performance using:

- on-time execution reliability;
- recurring exception causes;
- documentation error rate;
- incident frequency and responsiveness.

Where supplier evidence is not available due to terminal/authority restrictions, UDB will rely on available handover documentation and internal records.

### 6.5 Critical supplier controls (approved list)

- For high-value custody, transport, and terminal handling, UDB uses only suppliers that are approved under this framework.
- Approved suppliers are reviewed at least annually (Tier B/C) and after material incidents; corrective actions are applied where required.
- Under NDA, UDB can confirm supplier categories and the level of controls applied for the customer's use case.
- Before the first high-value shipment, UDB will issue a written supplier assurance letter (under NDA) covering: supplier categories used for the customer's lane (e.g., trucking/warehouse/handler/security), the due diligence tier (A/B/C), and the specific controls applied for the use case.

## 7. Approval, contracting, and onboarding outcome

Supplier onboarding outcomes may include:

- Approved (Tier A/B/C) — supplier may be used subject to operational feasibility;
- Approved with conditions — use is permitted only under stated constraints (e.g., limited commodities/routings);
- Pending — additional information required before approval;
- Rejected — supplier cannot be used due to risk/compliance issues.

Approval under this framework does not guarantee use on every shipment. Operational selection remains subject to routing feasibility, carrier/terminal constraints, and customer requirements.

## 8. Re-assessment and monitoring

UDB re-assesses suppliers using:

- periodic review (typically at least annually for Tier B/C where feasible); and/or
- event-driven review, triggered by:
- security incidents (theft/tampering allegations);
- repeated operational failures or material SLA breaches;
- compliance/sanctions changes or adverse media alerts;
- ownership/management changes or license lapses;
- regulatory or authority concerns.

UDB may suspend a supplier pending review where risk is material.

## 9. Red flags and escalation (stop/go discipline)

UDB escalates to Compliance (and may suspend use) if any of the following occurs:

- confirmed sanctions/restricted party hit;
- refusal to provide basic identity/license evidence (where reasonable);
- repeated theft/shortage allegations with unresolved evidence concerns;
- suspicious documentation behavior or integrity concerns;

- material safety or DG compliance failures;
- inability to provide minimal handover proof for custody services.

Decisions may include: continued use, restricted use, suspension, or termination.

## 10. Recordkeeping and retention

UDB retains due diligence records and supporting evidence for operational and compliance purposes, typically at least 5 years, unless a longer period is required by law or business need.

## 11. Limitations and no legal advice

This framework describes UDB’s internal due diligence approach and does not constitute legal advice. UDB may not be able to obtain all information for all suppliers due to market structure (e.g., authority-run terminals) or operational constraints. UDB applies reasonable, risk-based efforts to maintain practical controls.

## 12. Contact

For supplier due diligence inquiries or onboarding requests, contact: compliance@udb.ae