RISK ASSESSMENT POLICY

Transcontinental Group International Limited

Effective Date: May 27, 2025

1. Purpose

This policy establishes the strategic and operational framework for systematically identifying, assessing, mitigating, and monitoring risks that could affect the business continuity and regulatory compliance of Transcontinental Group International Limited. As a global freight forwarding and logistics company, we are committed to conducting business that is secure, ethical, and compliant with international standards and applicable laws.

The objectives of this policy include:

- Promoting risk-aware decision-making across all levels of the organization.
- Ensuring the safety, legality, and efficiency of our freight forwarding operations.
- Minimizing exposure to operational, regulatory, financial, reputational, and cyber risks.
- Ensuring compliance with international regulations and national laws, including but not limited to:

    - Hong Kong: Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), Strategic Commodities Control System

    - United States: Bank Secrecy Act (BSA), Office of Foreign Assets Control (OFAC) sanctions, Export Administration Regulations (EAR)

    - European Union: EU Dual-Use Regulation, EU Sanctions List, General Data Protection Regulation (GDPR)

- Other jurisdictions: Applicable customs, AML, and export control regimes

2. Scope

This policy applies to all business units, personnel, contractors, and third-party service providers engaged in:

- Air, sea, and land freight forwarding services
- Customs brokerage and clearance
- Warehouse management and goods distribution
- Customer onboarding and ongoing business relationships
- Handling, transportation, and storage of restricted, high-risk, or dual-use cargo
- Information management systems related to logistics operations

The policy is also applicable during subcontracting or transshipment procedures and governs the selection and monitoring of business partners globally.

3. Definitions

- Risk: The potential for an adverse outcome resulting from internal or external vulnerabilities affecting operations, compliance, or reputation.
- Risk Assessment: A structured approach to identifying, analyzing, and prioritizing risks.
- Risk Mitigation: Preventive or corrective measures taken to reduce the likelihood or impact of identified risks.
- High-Risk Cargo: Items such as weapons, dual-use goods, strategic commodities, or any goods that are subject to international sanctions or require specific licenses or end-user certificates.
- Third-Party Risk: Risk arising from vendors, clients, carriers, or partners that could compromise regulatory obligations or supply chain security.

4. Risk Categories

We assess risks in the following categories using qualitative and quantitative criteria:

- Operational Risk: Disruptions to freight movement, lost or damaged shipments, routing issues, port closures, strikes, or weather-related delays.
- Compliance Risk: Breach of customs regulations, trade embargo violations, shipment of sanctioned items, failure to conduct customer due diligence (CDD), or insufficient end-use verification.
- Financial Risk: Monetary losses due to cargo damage, claims, contract breaches, regulatory fines, or fraud.
- Reputational Risk: Negative media exposure or loss of stakeholder confidence resulting from illegal or unethical shipments.
- Cybersecurity Risk: Unauthorized access to cargo tracking systems, theft of client information, malware attacks, or ransomware targeting logistics data.
- Geopolitical Risk: Changes in trade policy, sanctions, or diplomatic relations affecting cargo movement.

5. Technical Execution of Risk Assessment

To ensure consistency, accountability, and effectiveness in identifying and mitigating risk, Transcontinental Group International Limited implements a standardized technical process for conducting risk assessments. This process applies across all operational areas, including freight movement, customer onboarding, cargo classification, and third-party partnerships.

Step 1: Risk Identification

- Collect relevant data from operational reports, incident logs, compliance checks, and external advisories (e.g., customs alerts, sanctions updates, geopolitical news).
- Identify risks related to cargo type (e.g., dual-use goods), customer profile (e.g., PEPs, sanctioned entities), destination countries, and mode of transport.
- Use red-flag indicators (e.g., incomplete end-user info, frequent transshipments) to flag potential high-risk transactions.

Step 2: Risk Categorization and Documentation

- Assign each identified risk to the appropriate category: Operational, Compliance, Financial, Reputational, Cybersecurity, or Geopolitical.
- Document the risk, source, and potential impact in the centralized Risk Register, including relevant details such as location, department, responsible parties, and associated shipments.

Step 3: Risk Analysis and Scoring

- Conduct a qualitative and quantitative analysis using a risk matrix that evaluates:
  - Likelihood (Low/Medium/High)
  - Impact (Low/Medium/High)
- Assign a risk score based on a predefined risk scoring system (e.g., 1–5 scale), generating a risk heat map for visual representation.
- For cyber and financial risks, integrate real-time system alerts and data analytics tools where applicable.

Step 4: Risk Prioritization

- Prioritize risks based on their scores.
- Critical/high-risk items are escalated to senior management and compliance officers for immediate review.
- Medium and low-risk items are logged and monitored for trend analysis or preventive mitigation.

Step 5: Mitigation Planning and Implementation

- Define risk mitigation strategies, which may include:
  - Enhanced due diligence (EDD)
  - Route or carrier changes
  - Customer re-screening
  - Licensing or end-use certification requests

- Technology upgrades or access controls (for cyber risks)

- Assign responsible teams to implement mitigation measures and document them in the Risk Register.

Step 6: Monitoring and Reporting

- Monitor risk indicators continuously through compliance software, internal audits, cargo monitoring tools, and employee feedback.
- Update the Risk Register regularly and review mitigation effectiveness in monthly compliance meetings.

Step 7: Review and Continuous Improvement

- Conduct a quarterly risk assessment review, incorporating lessons learned from incidents, industry trends, and regulatory changes.
- Revise procedures, controls, and risk thresholds as needed to maintain a proactive and adaptive risk management framework.

Approved by:

Evgeny Lerner
Chief Compliance Officer
May 27, 2025

Alexander Tsudikman
Director
May 27, 2025