dun & bradstreet

WHITEPAPER

Building Risk-Based Trade Governance In India Under FEMA 2026

July 2026

Executive summary

India's Foreign Exchange Management (Export and Import of Goods and Services) Regulations, 2026 ("FEMA 2026") marks a meaningful shift in the governance of cross-border trade transactions. It gives Authorised Dealer (AD) banks greater discretion in handling export and import transactions but also places greater responsibility on them to satisfy themselves about transaction genuineness, monitor export/import entries, and establish comprehensive internal policies and Standard Operating Procedures (SOPs). The practical implication is clear: banks are no longer only required to follow prescribed rules; they must also demonstrate that their own risk decisions are proportionate, consistent and defensible.

This changes the central control question for banks. The issue is no longer simply whether a transaction falls above or below a fixed regulatory threshold. The more important question is whether the bank can explain why a particular level of due diligence was sufficient for that transaction, that counter-party, that jurisdiction and that customer relationship.

This is particularly relevant for advance import remittances, new overseas suppliers, merchanting trade transactions, third-party payments, delayed import settlements, opaque ownership structures and transactions involving jurisdictions with higher secrecy, tax, sanctions or transparency risks. In such cases, trade documents may explain the stated commercial purpose of a transaction, but they may not always establish the credibility, operating capacity, ownership profile or financial standing of the overseas counter-party.

The next phase of trade-risk management will therefore require banks to move from document collection to evidence architecture: a clearer view of what evidence is needed, when counter-party intelligence should be refreshed, how jurisdiction risk should influence review, and how exceptions should be documented.

The objective is proportionality. Legitimate, low-risk trade should not face unnecessary friction, while large, unfamiliar, opaque or higher-risk transactions should be supported by stronger evidence. Banks that build calibrated frameworks will be better positioned to support trade growth while maintaining a defensible control environment.

From regulatory prescription to institutional accountability

Cross-border trade finance places banks in a dual role. They enable commerce by processing payments, supporting imports and exports, facilitating working capital and helping customers access global markets. At the same time, they act as control points in the foreign exchange system, responsible for ensuring that transactions are genuine, documented and consistent with regulatory expectations.

FEMA 2026 sharpens this control role. AD banks must satisfy themselves about the genuineness of export and import transactions before crediting or debiting customer accounts and before updating or closing entries in Export Data Processing and Monitoring System (EDPMS) or Import Data Processing and Monitoring System (IDPMS). They must also maintain comprehensive internal policies and SOPs for export/import transactions and merchanting trade transactions.

The practical shift is from regulatory prescription to institutional accountability. Banks may define their own thresholds, evidence requirements and escalation triggers, but those choices must be proportionate, consistently applied and defensible. The question is therefore not only whether a transaction meets a prescribed rule, but whether it meets the bank's own risk standards.

This creates an important operating challenge. Not every transaction presents the same level of risk, and not every overseas counter-party requires the same level of scrutiny. A payment to a long-established supplier with a proven trading history may warrant a different approach from an advance payment to a newly identified supplier with whom neither the customer nor the bank has previously transacted.

Transaction value is an obvious consideration, but value alone is rarely a reliable measure of trade risk. A lower-value advance to a newly established overseas supplier with limited transparency may present greater uncertainty than a higher-value payment to a known counter-party with a strong operating track record.

This means internal thresholds should not be viewed as standalone monetary limits. They should operate within a broader risk framework that considers factors such as, but not limited to:

- Customer relationship and trading history
- Counter-party familiarity and prior performance
- Ownership transparency and beneficial ownership visibility
- Jurisdiction characteristics and corporate disclosure standards
- Product or commodity risk
- Transaction structure and payment terms
- Availability of independently verifiable corporate information
- Adverse media, legal proceedings or other risk indicators

The strategic question is therefore: what combination of risk factors should determine when enhanced due diligence is required?

Why trade documents are necessary but not sufficient

Trade finance has traditionally relied heavily on documents. Invoices, purchase orders, contracts, shipping bills, bills of entry, transport documents, declarations and customer requests are central to establishing the stated commercial basis of a transaction.

These documents remain essential. They provide transaction evidence.

However, transaction evidence is not the same as counter-party evidence.

An invoice may show what is being purchased. It may not show whether the supplier is operationally active. A purchase order may show commercial intent. It may not show whether the counter-party has the capacity to fulfil the order. A registration document may show that an entity exists. It may not show whether the entity is newly incorporated, financially weak, controlled through nominees, linked to another group, or recently subject to adverse events.

This is particularly important in advance remittances. When payment is made before goods or services are received, the bank is effectively allowing funds to move out based on the anticipated future performance of an overseas counter-party. The quality of the counter-party therefore matters.

A mature trade-risk framework should distinguish between three types of evidence:

1) **Transaction evidence**

   This includes invoices, contracts, purchase orders, shipping documents, bills of entry and remittance requests.

2) **Customer evidence**

   This includes the Indian customer's banking history, account conduct, credit profile, trade track record and prior closure behaviour.

3) **Counter-party evidence**

   This includes the overseas company's identity, operating status, ownership structure, financial standing, business history, payment behaviour and adverse-event profile.

Many banks are already strong on transaction evidence and customer evidence. The more difficult discipline is counter-party evidence, because trade-based risk can hide in the space between what the documents say and what the counter-party actually is.

The counter-party visibility gap

The central issue in cross-border trade is that the overseas counter-party sits outside the bank's normal visibility perimeter. In many cases, the difficulty is not identifying the overseas counter-party. It is understanding who ultimately owns or controls it.

At first glance, this may appear to be a straightforward exercise. A supplier provides incorporation documents, a registration number, an address and banking details. The legal entity can be identified, and the transaction can be linked to a named counter-party.

In practice, however, legal ownership and economic control are often not the same thing. The immediate shareholder may not be the ultimate owner. The legal owner may not be the controlling party.

These distinctions matter because banks are not assessing documents in isolation. They are ultimately assessing whether the party receiving or sending funds is consistent with the stated commercial purpose of the transaction.

Consider the example below.

A direct shareholder (P1) owns 30% of Company C1. A second individual (P2) owns 100% of Company C2, which in turn owns 70% of Company C1.

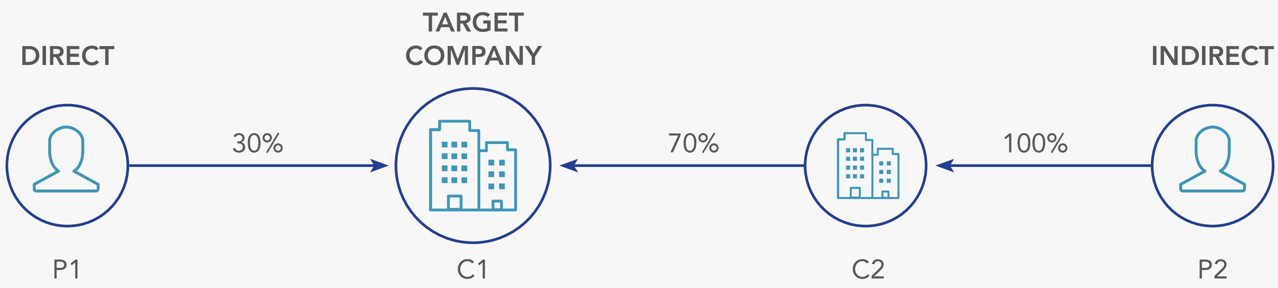
Although P2 does not appear as a shareholder of C1, P2 ultimately controls a 70% interest through indirect ownership.

The legal ownership structure is straightforward. Identifying the ultimate owner requires tracing ownership through multiple entities.

In practice, these structures may involve multiple layers across different jurisdictions rather than a single intermediary company. With each additional layer, ownership transparency declines and the effort required to establish ultimate ownership increases.

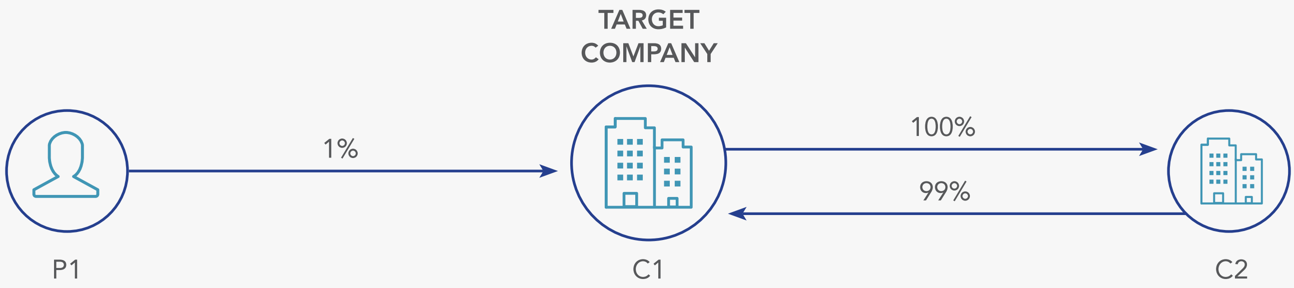
However, indirect ownership is only part of the challenge.

Example 1: Direct Versus Indirect Ownership



dun & bradstreet

Example 2: Looping Ownership



Ownership percentages can sometimes create a misleading picture of control.

Consider a structure where an individual (P1) owns only 1% of Company C1. At first glance, this may appear insignificant. However, C1 owns 100% of Company C2, while C2 owns 99% of C1. In effect, P1 may be the only natural person outside the loop and may ultimately benefit from the structure despite holding only a small direct stake.

This illustrates why shareholding percentages alone may not be sufficient to identify the Ultimate Beneficial Owner (UBO). Someone with less than 1% of total shareholding could still have meaningful control depending on the ownership and voting structure.

Ownership structures become particularly challenging when they involve:

- Indirect ownership through multiple entities
- Circular or looping ownership arrangements
- Nominee shareholders
- Trusts or holding companies
- Ownership spread across several jurisdictions
- Entities with limited public disclosure requirements

The challenge for banks is that these structures are not inherently unusual or improper. Many serve legitimate commercial, tax, investment, or corporate governance purposes. However, they make it substantially harder to determine who ultimately owns, controls or benefits from the transaction counter-party.

For banks operating under FEMA 2026, the implications are significant. The objective is not to investigate every overseas counter-party exhaustively. Rather, it is to recognise when ownership complexity becomes material to the risk assessment.

When ownership structures become unusually layered, indirect, or difficult to explain, the question is no longer simply: "Who is the counter-party?". Instead, it becomes: "Who ultimately owns or controls the counter-party, and do we understand that well enough to be comfortable with the transaction?"

That distinction often determines whether a transaction is merely documented – or genuinely understood.

Converting jurisdiction flags into evidence standards

Jurisdiction risk is often treated through public lists: blacklists, greylists, tax haven lists, sanctions lists, high-risk country classifications, or internal country-risk matrices. These are important inputs, but they are not always sufficient for trade-risk decisioning.

Public lists have three practical limitations.

First, they can be inconsistent. Different agencies may classify jurisdictions differently depending on whether the focus is tax transparency, Anti-Money Laundering (AML)/ Combating the Financing of Terrorism (CFT) risk, sanctions exposure, regulatory cooperation or financial secrecy.

Second, they can be incomplete. A jurisdiction may not appear on a high-risk list but may still present specific transparency challenges, such as limited beneficial ownership information, weak filing requirements, lack of public financial statements, or low availability of verified corporate records.

Third, they can be too blunt for operational use. A binary country flag can answer the question, "Should we be concerned about this jurisdiction?" It may not answer the more useful question for a bank: "How concerned should we be, and what additional evidence should be required?"

For banks, the requirement is not a simple yes/ no outcome. It is a usable risk signal that can be embedded into the SOP and reflected in evidence standards.

A more effective jurisdiction-risk framework should consider:

- Transparency of company registries
- Availability of beneficial ownership information
- Corporate disclosure standards
- Financial reporting requirements
- Quality of public records
- Tax haven or offshore financial centre characteristics
- Sanctions and AML/CFT exposure
- Legal enforceability
- Insolvency transparency
- Reliability of local corporate data
- Relevance to the specific trade corridor

The objective is not to label every low-tax or offshore jurisdiction as problematic. It is to identify where jurisdiction characteristics increase the need for counter-party evidence.

For example, an advance remittance to a supplier in a jurisdiction with limited corporate transparency may not be prohibited. But the bank may reasonably require stronger evidence of the supplier's identity, ownership, operating credibility and performance capacity.

Reducing judgement variability in trade risk decisions

In a principles-based regime, one of the biggest risks is not the absence of policy. Most banks will have a policy. The real risk is inconsistent judgement.

A branch in one region may process a transaction with basic documents, while another branch escalates a similar transaction for enhanced review. One relationship manager may treat a repeat supplier as low risk because the customer is known, while another may ask for updated counter-party verification because the supplier has not been reviewed recently. One operations team may focus on document completeness, while another may examine the commercial reasonableness of the transaction.

This inconsistency creates governance risk.

From a customer perspective, it creates unpredictability. From a compliance perspective, it creates weak defensibility. From a senior management perspective, it creates uncertainty about whether the bank's stated policy is being translated into consistent practice.

FEMA 2026 makes this more important because banks are required to have documented internal policies and SOPs covering trade transactions, approvals, delegations, extensions, advance payments and escalation processes.

A good SOP should therefore do more than list documents. It should define decision logic.

It should tell frontline, operations, trade, risk and compliance teams:

- When standard due diligence is sufficient, and when enhanced counter-party review is required
- When jurisdiction or counter-party risk should change the evidence requirement
- When senior approval, Letter of Credit or guarantee protection should be considered
- How repeat counterparties, exceptions and unresolved or delayed import/export entries should be handled

The objective is to reduce judgement variability without eliminating risk-based judgement.

From periodic checks to continuous counter-party intelligence

For AD banks, the more durable response to FEMA 2026 is not to create rigid evidence tiers or fixed external-data triggers. Those decisions must remain within each bank's own policy, risk appetite and governance framework. The stronger opportunity is to build a continuous monitoring capability that gives trade, operations, risk and compliance teams a more current and reliable view of overseas counterparties.

This matters because counter-party risk is not static. A supplier that appeared credible at onboarding may experience ownership changes, financial deterioration, insolvency events, adverse media, sanctions exposure, operating-status changes or changes in group linkage over time. A point-in-time review may therefore be sufficient to support an initial decision, but it may not be sufficient to support repeated trade activity over an extended period.

Technology-enabled monitoring can help banks move from episodic checks to an intelligence-led operating model. By drawing on timely, accurate and reliable data sources that bring together corporate identity, operating status, ownership, global linkage, adverse events, financial indicators and jurisdiction-level signals, banks can develop a more complete view of counterparties and trading relationships.

This does not mean outsourcing the bank's judgement. The bank remains responsible for its own decisioning, approvals, thresholds and regulatory compliance. External business intelligence should instead support the bank's internal judgement by improving the quality, consistency and timeliness of the evidence available to decision-makers.

A continuous monitoring approach may help banks strengthen trade governance in three practical ways.

- It builds a unified counter-party view by connecting legal identity, ownership, group linkage, operating status and business activity.
- It improves consistency by giving trade, operations, risk and compliance teams a common evidence base.
- It enables timely review when material changes occur across repeat trading relationships, including ownership shifts, adverse events, insolvency indicators, sanctions exposure or deterioration in business standing.

The value of such an approach depends heavily on data quality. For banks, the relevant question is not only whether information is available, but whether it is verified, current, traceable and sourced through a reliable and transparent data supply chain. In cross-border trade, where counterparties may sit across jurisdictions with different disclosure standards, the credibility of the data source becomes central to the credibility of the review.

A trusted third-party data provider can therefore play an important enabling role, provided the bank uses such information as one input within its own risk framework. Reliable corporate linkage, ownership intelligence, adverse-event monitoring and jurisdiction-risk signals can help banks build a more unified view of overseas counterparties.

Over time, this can help banks move beyond compliance as a box-ticking obligation. The benefit is not merely regulatory comfort. It is better trade governance: faster recognition of legitimate repeat relationships, sharper escalation where risk signals change, more consistent application of internal policy, and stronger defensibility when decisions are reviewed after the event.

Conclusion: Building a defensible trade governance model

FEMA 2026 does not prescribe a single due diligence model for all banks. By giving AD banks greater discretion, it makes each bank's own trade-risk architecture more important: how it assesses transaction genuineness, sets thresholds, evaluates overseas counterparties, adjusts for jurisdiction risk and documents exceptions.

The strongest response will not be a heavier checklist. It will be a more intelligent, evidence-led framework.

A future-ready AD bank should be able to answer four questions for every material trade-risk decision:

1) Was the transaction commercially coherent?
2) Was the counter-party sufficiently understood?
3) Was the level of due diligence proportionate to the risk?
4) Can the decision be defended after the event?

If the answer to all four is yes, the bank is not merely complying with FEMA 2026. It is building a stronger model for cross-border trade governance.

The competitive advantage in trade finance will increasingly belong to banks that can combine speed with defensibility. Faster processing will matter, but not at the cost of weak evidence. Stronger controls will matter, but not if they create unnecessary friction for legitimate trade. The effectiveness of risk-based trade governance will increasingly depend on access to reliable counterparty intelligence from providers with a broad global presence, helping banks build a more complete and defensible view of overseas trading relationships. The winning model will be risk-based, intelligence-led and operationally usable.

ABOUT DUN & BRADSTREET®

Dun & Bradstreet, a leading global provider of business decisioning data and analytics, enables companies around the world to improve their business performance. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to accelerate revenue, lower cost, mitigate risk and transform their businesses. Since 1841, companies of every size have relied on Dun & Bradstreet to help them manage risk and reveal opportunity. For more information on Dun & Bradstreet, please visit www.dnb.com.

Dun & Bradstreet Information Services India Private Limited is headquartered in Mumbai and provides clients with data-driven products and technology-driven platforms to help them take faster and more accurate decisions across finance, risk, compliance, information technology and marketing. Working towards Government of India's vision of creating an Atmanirbhar Bharat (Self- Reliant India) by supporting the Make in India initiative, Dun & Bradstreet India has a special focus on helping entrepreneurs enhance their visibility, increase their credibility, expand access to global markets, and identify potential customers & suppliers, while managing risk and opportunity.

India is also the home to Dun & Bradstreet Technology & Corporate Services LLP, which is the Global Capabilities Center (GCC) of Dun & Bradstreet supporting global technology delivery using cutting edge technology. Located at Hyderabad, the GCC has a highly skilled workforce of over 500 employees, and focuses on enhanced productivity, economies of scale, consistent delivery processes and lower operating expenses.

Visit www.dnb.co.in for more information.