THEMIS

India

COUNTRY RISK BRIEFING - 2025

WWW.WEARETHEMIS.COM

Country Overview

Location:
South Asia, bordered by Pakistan, China, Nepal, Bhutan, Bangladesh, and Myanmar; surrounded by the Indian Ocean

Capital:
New Delhi

Currency:
Indian Rupee (₹, INR)

Population:
Approximately 1.46 billion (2025 UN estimate); most populous country in world

Unemployment Rate:
4.2% (2024 World Bank estimate)

GDP:
Ranked 5th globally; nominal GDP approximately $3.91 trillion (2024 World Bank estimate)

Major Economic Sectors:
Information technology and services, agriculture, manufacturing, telecommunications, pharmaceuticals, textiles, and renewable energy

Natural Resources:
Coal, iron ore, bauxite, natural gas, oil, arable land, minerals, forests, solar and wind energy potential

Government:
Federal parliamentary democratic republic; a Commonwealth member country

Economy & Politics

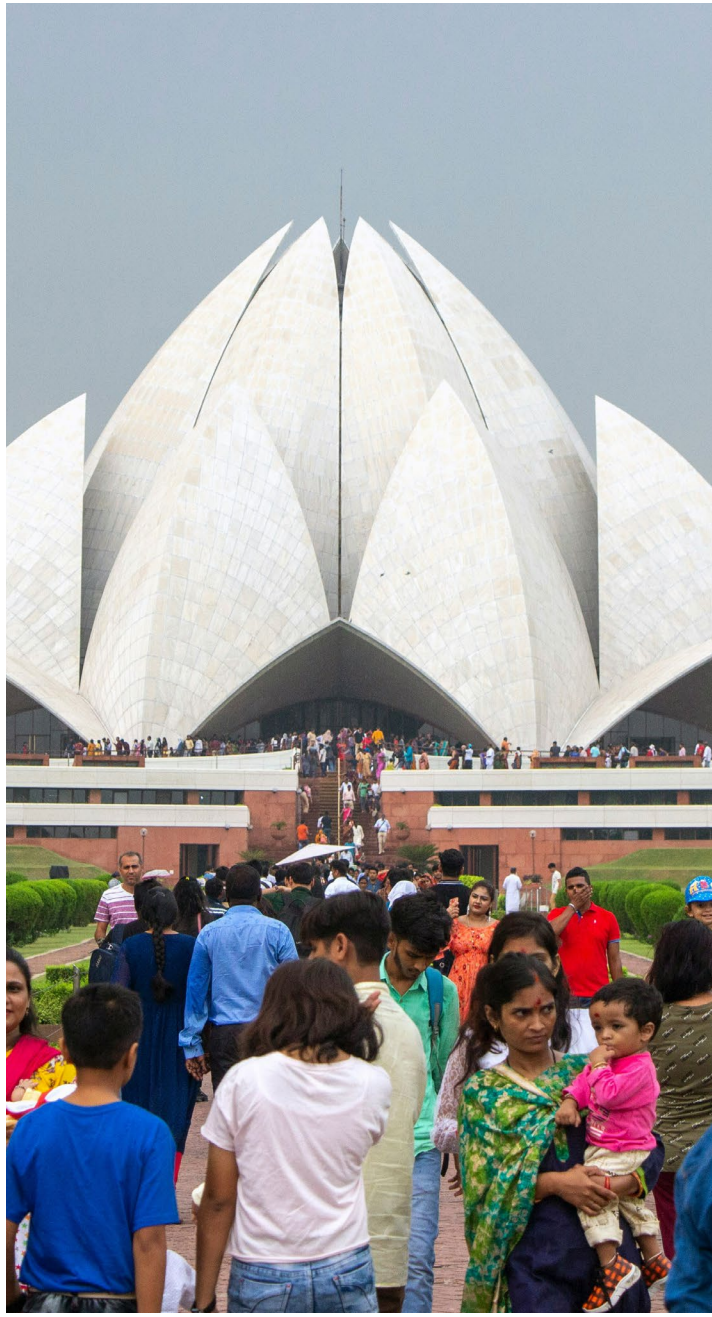
India is the world's most populous democracy and one of the largest emerging markets, playing a pivotal role in the global economy as both a major consumer base and a key production and trade hub. With a GDP estimated at $3.91 trillion USD in 2024, it ranks as the fifth-largest economy by nominal terms and remains one of the fastest-growing among G20 nations. Growth is driven by sectors such as information technology, business process outsourcing, telecommunications, and financial services—all benefiting from global integration and rapid digital adoption.

While India ranks 63rd out of 190 in the World Bank's Ease of Doing Business Index (2020), challenges persist around contract enforcement, infrastructure, and regulatory complexity. Structural risks also stem from a large informal economy, inflation volatility, and supply chain vulnerabilities. Government initiatives like Digital India, Make in India, and Startup India are seeking to modernise the economy, promote manufacturing, and expand financial inclusion.

India's trade footprint is broad and expanding, with key partners including the US, China, UAE, the EU, and ASEAN. Imports are dominated by crude oil, electronics, machinery, and gold, while exports include refined petroleum, pharmaceuticals, textiles, IT services, and agricultural products. Efforts to diversify trade ties and attract foreign investment have led to new bilateral agreements and expanded supply chain networks—raising the bar for compliance with international AML and sanctions frameworks, particularly in high-risk jurisdictions.*

Politically, India is a federal parliamentary republic with executive power held by the Prime Minister and a bicameral legislature. The Constitution guarantees fundamental rights, separation of powers, and an independent judiciary. States and Union Territories exercise considerable autonomy in specific areas, often complicating regulatory enforcement. On the global stage, India is an influential player in the G20, BRICS, the Quad, and UN bodies. However, geopolitical tensions with China and Pakistan, along with internal pressures from regional and communal divisions, continue to shape its domestic and foreign policy environment.

** Please note that while trade and export data are correct at the time of writing, they should be interpreted with caution, as ongoing shifts in US tariff policies may significantly impact global trade dynamics and data reliability in the near term.*



Themis Expert View

WRITTEN BY:

Eliza Thompson
Financial Crime Researcher

India's geographic and political positioning places it at the crossroads of major transnational financial and trade flows—both legitimate and illicit. With busy maritime routes in the Indian Ocean and porous land borders with countries like Pakistan, Nepal, and Myanmar, the country is a natural transit and destination point for a wide range of financial and predicate crimes. Illicit trade is a particular concern, especially given India's role in global supply chains and its large volume of imports and exports. Informal remittance systems like hawala, which operate outside formal banking channels, also remain a persistent challenge despite regulatory scrutiny. These risks are amplified by India's strong financial and trade ties with the Gulf, Southeast Asia, and parts of Africa—regions that often face their own vulnerabilities in tackling financial crime.

For financial institutions and businesses operating in India, this environment demands heightened vigilance.

The complex and international nature of illicit finance in the country means that standard compliance procedures may not be sufficient. Firms must go beyond basic due diligence to include deep screening of counterparties, robust beneficial ownership checks, and ongoing network mapping to identify hidden connections that could expose them to risk. With sophisticated actors often using layered structures, proxy entities, and legitimate-seeming trade routes to mask the movement of illicit funds, companies need to ensure that their compliance programs are both locally informed and globally integrated. Moreover, inconsistent enforcement and varying regulatory maturity across India's states require businesses to maintain flexible, risk-sensitive approaches rather than relying solely on formal legal protections. In this context, proactive risk assessment and continuous monitoring become essential for avoiding exposure to financial crime and regulatory penalties.

Regulatory Overview

Primary Anti-Financial Crime Regulators and Agencies:

- **Financial Intelligence Unit – India (FIU-IND):** Under the Ministry of Finance, the FIU receives, analyses, and disseminates Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), and other reports from reporting entities.
- **Enforcement Directorate (ED):** A law enforcement agency under the Department of Revenue, Ministry of Finance, the ED investigates and prosecutes money laundering and foreign exchange violations under the PMLA and FEMA (Foreign Exchange Management Act), respectively.
- **Directorate of Revenue Intelligence (DRI):** An intelligence and enforcement agency, the DRI investigates smuggling, customs evasion, and trade-based financial crimes.
- **Central Bureau of Investigation (CBI):** India's premier investigative agency, the CBI handles major financial crimes including bank frauds, corruption, and economic offenses involving public sector entities, often overlapping with money laundering investigations.
- **Reserve Bank of India (RBI):** The RBI is India's central bank and the primary regulator for banks, non-banking financial companies (NBFCs), and payment system operators. It is also an AML/CFT supervisor under the Prevention of Money Laundering Act (PMLA), 2002.
- **Securities and Exchange Board of India (SEBI):** The regulator for the securities and capital markets, the SEBI supervises stockbrokers, mutual funds, portfolio managers, and other market intermediaries for AML/CFT compliance under the PMLA.
- **Insurance Regulatory and Development Authority of India (IRDAI):** The IRDAI regulates the insurance sector and ensures AML/CFT compliance by insurance companies as per PMLA obligations.
- **Serious Fraud Investigation Office (SFIO):** Under the Ministry of Corporate Affairs, SFIO investigates complex corporate frauds, including money laundering and accounting irregularities.
- **Central Board of Direct Taxes (CBDT) and Central Board of Indirect Taxes and Customs (CBIC):** The CBDT investigates tax evasion and illicit financial flows; involved in financial crime enforcement and the CBIC includes Customs and GST departments, involved in trade-based money laundering and black money investigations.
- **Ministry of External Affairs – Sanctions Division:** The Ministry of External Affairs' Sanctions Division implements and coordinates India's adherence to international sanctions (including those from the UN Security Council).

Regulatory Overview

Primary Anti-Financial Crime Legislation:

- **Prevention of Money Laundering Act, 2002 (PML):** The PML is the primary legislation that criminalises money laundering and mandates reporting, record-keeping, and investigation of suspicious financial activities by designated entities.
- **PML (Maintenance of Records) Rules, 2005:** This legislation requires reporting entities to maintain records of transactions and CDD records.
- **PML (Amendment) Act, 2012:** The objective of this amendment is to further strengthen the AML framework by clarifying and enhancing provisions—including lowering the threshold for identification of beneficial owners, introducing the concept of politically exposed persons (PEPs), and expanding the scope of reporting entities to include non-profit organisations.
- **PML (Amendment) Act, 2015:** This amendment was made to align Indian AML laws with international standards, thus bridging gaps and enhancing transparency by introducing the concepts of "reporting financial institution" and "reporting authority".
- **PML (Maintenance of Records) Amendment Rules, 2023:** This amendment mandates reporting entities to disclose beneficial owners and imposes stricter KYC norms for professionals like chartered accountants and company secretaries—and extends AML measures to include cryptocurrency and virtual digital asset (VDA) transactions.
- **Bharatiya Nyaya Sanhita, 2023:** A recent criminal code, replacing the Indian Penal Code (PIC), aiming to modernise and reform the criminal justice system by more effectively addressing offences such as organised crime, cyber offences, and offences against women and children.
- **Foreign Exchange Management Act, 1999 (FEMA):** Regulates foreign exchange transactions and cross-border financial flows to prevent capital flight and illicit remittances.
- **Reserve Bank of India Act, 1934:** Establishes the RBI's regulatory authority over banks and financial institutions, including issuing AML/CFT guidelines.
- **Securities and Exchange Board of India Act, 1992:** Empowers SEBI to regulate the securities market and combat market abuse, fraud, and insider trading.
- **Companies Act, 2013:** Sets governance standards for companies and provides enforcement mechanisms against corporate fraud and financial misconduct.
- **Prevention of Corruption Act, 1988 (amended 2018):** Criminalises bribery and corruption involving public officials and introduces liability for commercial organisations.
- **Unlawful Activities (Prevention) Act, 1967 (UAPA):** Targets the financing of terrorism by criminalizing support for banned organisations and allowing asset freezes.
- **Customs Act, 1962 & GST Acts:** Empower authorities to detect and penalize smuggling, tax evasion, and trade-based financial crime through indirect tax systems.

Financial Action Task Force Assessment

India's 2024 joint FATF-APG-EAG Mutual Evaluation found that the country has achieved a high level of technical compliance with FATF Recommendations and has made notable progress in implementing measures to combat money laundering and terrorist financing. The report highlights India's strengths in financial inclusion, use of financial intelligence, beneficial ownership access, international cooperation, and asset recovery. Authorities demonstrate good coordination and understanding of risk, particularly in the financial sector, and are effectively disrupting criminal activities.

The evaluation does note, however, key areas requiring further attention and improvement, including the need to conclude money laundering and terrorist financing prosecutions, enhance supervision of non-financial sectors and virtual asset service providers, and improve outreach to non-profit organisations through a risk-based approach. India must also strengthen implementation of cash restrictions in high-risk sectors, expand coverage of domestic PEPs, and ensure consistent application of preventative measures across all reporting entities. As the world's most populous country and a major emerging economy, India faces ongoing threats from fraud, corruption, drug trafficking, and terrorism, and will report back to the FATF Plenary in 2027 as part of the regular follow-up process.

Category	2024 FATF Mutual Evaluation
Overall Assessment	India was placed in "regular follow-up", with the FATF finding that it had achieved a high-level of technical compliance across the FATF Recommendations and had taken significant steps to implement measures to tackle illicit finance. Nevertheless, the FATF found that it was critical for the country to continue to improve its system as its economy and financial system carry on growing.
Technical Compliance Ratings	**Compliant:** 11 **Largely Compliant:** 26 **Partially Compliant:** 3 • R.8 - Non-profit organisations • R.12 - Politically Exposed Persons • R.28 - Regulation and Supervision of DNFBPs
Key Risks Identified	- Main money laundering risks originate from illegal activities within the country, primarily cyber-enabled fraud and other forms of fraud, corruption, and drug trafficking. - India faces serious terrorism and terrorist financing threats, including related to ISIL or Al Qaeda.
Strengths	- India has a strong emphasis on prevention and disruption and has demonstrated a strong ability to conduct complex financial investigations. - India has made significant steps in financial inclusion and transparency, which in turn contributes to AML/CFT efforts. - Authorities have a comprehensive understanding of the money laundering, terrorism, and proliferation financing risks in the country. - There is good understanding of risk and the application of preventative measures in the financial sector, especially by commercial banks, although less so by some other smaller financial institutions. - Authorities cooperate and coordinate effectively on matters relating to illicit financial flows, including the use of financial intelligence, and achieve positive results in asset recovery and implementing targeted financial sanctions.
Areas for Improvement	- India treats some predicate crimes, such as fraud, in line with money laundering risks but could do a better job with other predicate offences, including human trafficking and drug trafficking. - India needs to address the issue of lack of coverage of domestic PEPs from a technical compliance perspective and ensure reporting entities fully implement these requirements. - Implementation of preventative measures by the non-financial sector and virtual asset service providers, and supervision of those sectors, is at an early stage. - The country should improve implementation of cash restrictions by dealers in precious metals and stones as a priority, given the materiality of the sector.

Financial Crime Risk Matrix

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Bribery & Corruption	Medium	FATF Mutual Evaluation 2024 The 2024 MER identified corruption as a key predicate crime in the country, in alignment with India's own NRA. Transparency International Corruption Perceptions Index 2024 see here* 38 / 100 (Ranked 96th of 180 countries) **Transparency International Corruption Perceptions Index score is the perceived level of public corruption, where 0 means highly corrupt and 100 means very clean.* Trace 2024 Bribery Risk Matrix see here* Rank 126th; Score 56 / 100 **Trace measures business bribery risk with a lower score indicating a lower bribery risk, while a higher score indicating a higher bribery risk.* Global Organized Crime Index 2023 see here* Government Transparency and Accountability: 5 / 10 State-Embedded Criminality: 6 / 10 Private Sector Criminality: 5 / 10 **Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.* Worldwide Governance Indicators 2023 see here* Control of Corruption: 41.51 / 100 **The WGI represent a country›s score and rank among all countries worldwide on each governance dimension.*	Infrastructure, Mining/Natural Resources, Construction, Defence, Public Procurement	Notable corruption exposure from foreign PEPs, multinational business; and sanctions exposure
Financial Secrecy	Medium	Financial Secrecy Index 2025 see here* Overall score: 56 / 100 (24th globally) **Secrecy index measures the level of financial secrecy, with 0 meaning no secrecy and 100 meaning maximum secrecy.*	Company & Trust Service Providers, Lawyers, Private Banking, Hawala	Exposure to offshore structures

Tax Crime	Medium	FATF Mutual Evaluation 2024 The 2024 MER identified tax crimes as a predicate crime as linked to abuse of beneficial ownership and offshore financial secrecy jurisdictions.	Corporate Entities, High-Net Worth Individuals, Lawyers	Exposure to offshore structures and transnational evasion networks
Arms Trafficking	Medium	Global Organized Crime Index 2023 see here* Arms Trafficking: 6 / 10 **Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.*	Illegal Markets	Significant risk due to porous borders and regional conflict and instability
Environmental Crime	Medium-High	Global Organized Crime Index 2023 see here* Flora Crimes: 6 / 10 Fauna Crimes: 7 / 10 Non-Renewable Resource Crimes: 2.5 / 10 **Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.*	Mining, Forestry, Other Non-Renewable Resources, Shipping and Transporation	Often links to transnational organised crime groups and sourced from third countries
Sanctions Evasion	High	India faces notable and growing sanctions exposure risk—primarily due to its ongoing strategic and economic engagements with Russia and Iran—but mitigates it through partial alignment with Western compliance norms.	Trade, Shipping, Infrastructure, Natural Resources, Defence-related Industries, Professional Services	Significant exposure due to high levels of trade with sanctioned countries and third-country jurisdictions
Fraud	High	FATF Mutual Evaluation 2024 The 2024 MER identified fraud as a key predicate crime in the country.	Financial Services, Technology, Social Media & E-Commerce, Telecoms	Cyber-enabled fraud has a strong transnational component in the country

* Methodology: Each financial crime risk rating is derived from a combination of globally recognised indices and supplementary risk factors. Each index score is normalised and translated into a Red-Amber-Green (RAG) rating. Specifically, jurisdictions or entities are grouped based on their position within the distribution of index values, with the top, middle, and bottom third of scores per index corresponding respectively to Green, Amber, and Red (e.g. a 5/10 rating in one index would be equivalent to a 12/24 rating in another). Additional risk factors — such as enforcement actions, FATF evaluations, and our own Themis internal intelligence — also influence the final RAG classification through an overlay and adjustment process.

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Cybercrime	High	FATF Mutual Evaluation 2024 The 2024 MER identified cyber-enabled crime as a key predicate crime in the country, in alignment with India's own NRA. Global Organized Crime Index 2023 see here* Cyber-Dependent Crimes: 7.5 / 10 **Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.*	Financial Services, Fintech, Telecoms, Data Services, Defence, Government Agencies, Public Infrastructure	Often transnational in nature, involving international organised criminal groups
Drug Trafficking	High	FATF Mutual Evaluation 2024 The 2024 MER identified drug trafficking as a key predicate crime in the country, in alignment with India's own NRA. Global Organized Crime Index 2023 see here* Heroin Trade: 7 / 10 Cocaine Trade: 3.5 / 10 Cannabis Trade: 7.5 / 10 Synthetic Drug Trade: 7 / 10 **Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.*	Trade, Shipping & Logistics, Pharmaceutical	Significant exposure via border regions, major transit and destination country
Modern Slavery & Human Trafficking	High	US Department of State 2024 Trafficking in Persons Report see here* Tier 2 **Tier 2 rating means the Government in question does not fully meet the minimum standards for the elimination of trafficking but is making significant efforts to do so.* Walk Free Global Slavery Index see here* Vulnerability: 56 / 100 Governance Response: 46 / 100 **Vulnerability score measures vulnerability to modern slavery with a greater score reflecting higher levels of vulnerability.* **Governance score measures government response to modern slavery with a higher score reflecting stronger government response.* Global Organized Crime Index 2023 see here* Human Trafficking: 8 / 10 Human Smuggling: 6.5 / 10 **Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.*	Domestic work, construction, hospitality	Migrant labour flows from Asia; abuse during recruitment, visas, or work permits

Areas of Financial Crime Vulnerability

- **Informal Financial Systems:** India's widespread use of hawala networks and unregulated money services businesses (MSBs) is often used to facilitate underground value transfers, trade settlement, and remittances. These channels are routinely exploited by criminal networks and terrorist financiers, both domestic and transnational.

- **Trade-Based Illicit Finance:** As a major global trading economy, India is vulnerable to trade-based money laundering (TBML) and other illicit trade activities, especially involving natural resource crimes, drug trafficking, and goods smuggling.

- **Sanctions Evasion and Dual-Use Goods:** India's extensive trade with countries under sanctions (e.g. Russia and Iran) increases exposure to sanctions circumvention, including via third-party intermediaries and dual-use goods exports with potential military or nuclear applications.

- **Geographic Exposure to Illicit Flows:** India shares porous borders with high-risk countries (Pakistan, Nepal, Bangladesh, Myanmar), exposing it to terrorist financing, smuggling, and cross-border criminal activity. Border regions are often used for trafficking and illicit fund movement.

- **Corruption and Abuse of Legal Structures:** Endemic corruption in sectors such as infrastructure, mining, and logistics, as well as in public procurement, creates elevated bribery, fraud, and transnational crime-linked risks. Widespread use of shell companies is common for hiding beneficial ownership and paying illicit commissions to PEPs and bureaucrats.

- **Offshore and Secrecy Jurisdictions:** Indian individuals and entities have been repeatedly named in offshore leaks (e.g. the ICIJ Panama, Paradise and Pandora Papers), revealing the use of tax havens for asset concealment, evasion, and laundering.

- **Cyber and Fraud Risks:** Rapid digitalisation and innovation has led to a surge in cyber-enabled fraud and identity theft, impacting the private sector and consumers, as well as the public sector via targeted attacks. Weak cybersecurity standards and inconsistent regulatory coverage exacerbate vulnerabilities.

- **Regulatory Gaps and Fragmented Supervision:** AML/CFT oversight is divided across multiple regulators (RBI, SEBI, IRDAI), leading to inconsistent enforcement and supervisory blind spots. DNFBPs (e.g. real estate agents, lawyers, accountants) remain largely outside formal AML supervision, despite being high-risk.

Financial Crime Risk In-Depth

01 Money Laundering: Medium-High Risk

India faces significant risks related to money laundering, driven in large part by its large informal economy, high levels of international trade and business, and vulnerabilities in financial oversight. The country's money laundering risks are primarily concentrated across fraud, trade-based schemes, the real estate and precious metals sectors, and trafficking and corruption related offences, and often involve the flow of illicit cross-border funds. While India has made significant progress in strengthening its AML framework—such as through regulatory measures by the Reserve Bank of India (RBI) and adoption of FATF recommendations—enforcement gaps, delays in prosecutions, and inconsistent reporting standards across sectors persist. Moreover, Indian entities' notable use of shell companies, offshore structures, and evolving fintech platforms continues to pose challenges for detection and control.

02 Bribery & Corruption: High Risk

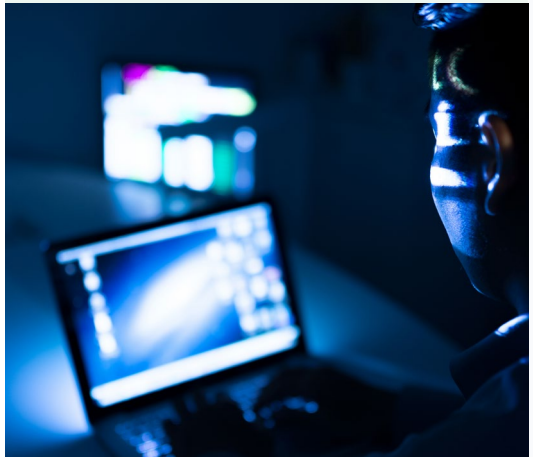
India faces bribery and corruption risks across both public and private sectors, driven in part by high levels of international business and political exposure, as well as regulatory challenges and weak enforcement in some areas. Corruption is present across multiple levels of government, affecting key areas such as public procurement and licensing, and is particularly rampant at lower levels of the government, judiciary, and bureaucracy. Corruption risks also significantly impact the private sector in India, where bribery and unethical practices can influence business operations, contracts, and regulatory compliance. The Global Organized Crime Index has noted that the nexus between corrupt contractors, politicians, local officials, and law enforcement leads to a range of predicate crimes such as trafficking and environmental crime risks. Additionally, corruption risks are often intertwined with international political dynamics and can overlap with risks linked to sanctions and geopolitical conflict.

03 Terrorist Financing: High Risk

India faces serious terrorist financing threats, both internally and externally. The country has long contended with terrorism linked to regional insurgencies and geopolitics, including cross-border terrorism from neighbouring Pakistan and from international terrorist organisations including ISIL and Al Qaeda. Terrorist financing in the country primarily involves a mix of formal financial channels, informal and hawala networks, cash couriers, and charitable organisations used as fronts. Despite a robust legal and law enforcement framework, challenges persist in detecting and disrupting complex financial flows that support terrorism. Moreover, digital payment service platforms, virtual assets, and emerging technologies have added new layers of complexity.

04 Sanctions Evasion: High Risk

India faces significant risks related to sanctions circumvention and violations due to its extensive trade relationships with sanctioned countries and entities, including Russia and Iran. The country's complex and diverse economic interactions, particularly in sectors like energy, technology, and finance, create risks of indirect involvement in sanctioned transactions. Additionally, gaps in regulatory oversight, inconsistent enforcement mechanisms, and the use of intermediaries or third-party jurisdictions heighten vulnerability when it comes to unintended violations and circumvention. These factors, along with shifting geopolitical dynamics and a constantly evolving global sanctions landscape, make it necessary for companies operating or trading in the country to maintain rigorous and ongoing sanctions compliance monitoring.



05 Drug Trafficking: High Risk

India faces high levels of drug trafficking exposure deriving from its geographical location. It is a major transit hub for opium thanks to its position between two large opium-cultivation regions: to its west, the Golden Crescent (Afghanistan, Pakistan, and Iran), and to its east, the Golden Triangle (Myanmar, Thailand, and Laos). The country also struggles with illegal domestic production of opium. Furthermore, India is a destination for cocaine trafficking—traditionally a smaller market—with smuggling led by criminal groups from Africa and, more recently, South America. Meanwhile, cannabis plays a central role in the country's illicit drug trade, with Odisha emerging as a major trafficking centre, particularly of cannabis grown in areas previously affected by the Maoist insurgency. India is also a source and transit point for synthetic drugs, with domestic use mostly confined to urban areas. The country is believed to be a secondary source of precursor chemicals, from where shipments pass to the Golden Triangle in Southeast Asia. The dark web has become a key driver of India's illicit drug trade, with the country used as a key transit route for drugs sold on major dark web marketplaces, as well as a source of diverted pharmaceuticals used by criminal networks for trafficking.

06 Fraud: High Risk

Fraud in India remains a significant challenge, with the FATF identifying fraud as the key predicate crime in the country. Common types of fraud include financial scams, corporate fraud, and cyber-enabled fraud, often facilitated by gaps in oversight and enforcement. The rise of digital transactions and online platforms has increased vulnerabilities to identity theft, phishing, and payment fraud. Experts have noted a rise in local criminal gangs engaging in fraud, with cities such as Delhi and Mumbai seeing sharp increases in fraud. Despite strengthening legal frameworks and regulatory bodies, inconsistent implementation and limited awareness continue to pose risks for businesses and individuals alike. Addressing fraud effectively requires enhanced transparency, robust internal controls, and greater collaboration between the government, financial institutions, and the private sector.

07 Cybercrime: High Risk

Cybercrime remains a major and growing threat in India, with cybercrime having surged in recent years. Rises in cybercrime have been fueled in large part by increased internet penetration and digital adoption, as well as a growing reliance on online services. The country faces a range of threats, including data breaches, ransomware attacks, financial fraud, identity theft, and phishing schemes. The country is among the top three countries worldwide most affected by ransomware attacks, with the majority of companies in India having experienced at least one ransom attack, and almost half suffering multiple attacks, according to the Global Organized Crime Index. Key sectors including banking, e-commerce, and education have been hit the hardest, as well as the public sector, with criminals targeting government infrastructure. Moreover, more than half of Indian adults have been affected by cyber-enabled financial crime. Challenges like inadequate cybersecurity awareness, limited skilled workforce, and fragmented regulatory frameworks exacerbate these risks.

08 Modern Slavery & Human Trafficking: High Risk

India plays a significant role in human trafficking across South Asia, grappling with a deeply entrenched and well-organised network operating both domestically and across borders. Women and children are often trafficked for sexual exploitation and forced labour, while men from Nepal and Bangladesh are predominantly trafficked into the country for the purposes of forced labour. Police corruption exacerbates this criminal market, and debt bondage is a common tactic used by traffickers to lure unemployed workers into forced labour in various industries. Porous borders in some regions and recent political conflicts in neighbouring countries have led to an increase in incidents of human smuggling, particularly involving those seeking refuge from Myanmar, with criminal networks often soliciting large sums of money to facilitate irregular migration into the country.

09 Arms Trafficking: Medium

India serves as a source, transit, and destination country for the illegal arms trade. According to the Global Organized Crime Index, Delhi is a crucial transit point for guns being trafficked across the country, predominately from central and eastern states to the north. Illegal arms factories have also grown across Delhi, and arms dealers based in Meerut, Aligarh, and other cities in western Uttar Pradesh are now the primary suppliers of illicit firearms demanded by criminals in the country. There is growing insecurity and violence in many cities because of the easy availability of illegal weapons, and illegal arms are closely linked to drug trafficking groups in the country.

10 Tax Crime: Medium Risk

Tax crime risks in India encompass a range of illicit activities designed to evade or avoid tax liabilities. Common offenses include income concealment, where individuals or businesses underreport earnings to reduce taxable income, and bogus billing, where fake or inflated invoices are used to falsely claim input tax credits under the Goods and Services Tax (GST) regime. Shell companies and benami transactions are often used to mask beneficial ownership and launder undeclared income. Cash-based transactions, particularly in sectors like real estate, construction, and jewelry, remain a significant source of black money and unreported income. Another widespread practice is misclassification of goods or services to take advantage of lower GST rates or exemptions. Businesses may also engage in round-tripping, where funds are cycled through offshore or related entities and brought back as foreign investments or loans to claim tax exemptions.

11 Financial Secrecy: Medium Risk

Financial secrecy crimes in India enable a range of other financial crimes, including tax evasion, money laundering, and illicit financial flows by obscuring the true ownership and movement of assets. Common methods include the use of shell companies, benami transactions (assets held in the name of another person), undisclosed offshore accounts, and complex trust structures. Despite reforms, such as the Benami Transactions Act and adoption of the Common Reporting Standard (CRS), enforcement gaps, weak beneficial ownership transparency, and fragmented oversight across agencies remain challenges. High-profile leaks like the Panama and Pandora Papers have highlighted India's vulnerability. Stronger disclosure norms, improved data sharing among regulators, and greater public transparency are essential to tackling these risks.

12 Environmental Crime: Medium-High Risk

India is exposed to a wide array of environmental crimes, often closely linked to related financial crimes. The country serves as a key hub for the illicit gold trade globally, for example, with hundreds of tonnes of illicit gold exiting India annually. A nexus of corruption officials and transnational criminals drives this trade, with the country serving as a hub for gold smuggled from conflict zones in Africa and South America. The illegal wildlife trade is also a considerable issue, with the country serving as both a source country for illegally poached animal products and a trafficking hub. Wildlife species and products commonly trafficked out of and through India include tiger and leopard skins, rhino horns, ivory, turtles, snakes, and caged birds. Flora crimes are also present in the country, including the illegal harvesting and trade of medicinal plants and non-timber forest products, which often involves illegal collection among local and tribal communities. India also faces risks related to other non-renewable resources, including sand trafficking.

Case Study

Gupta Brothers

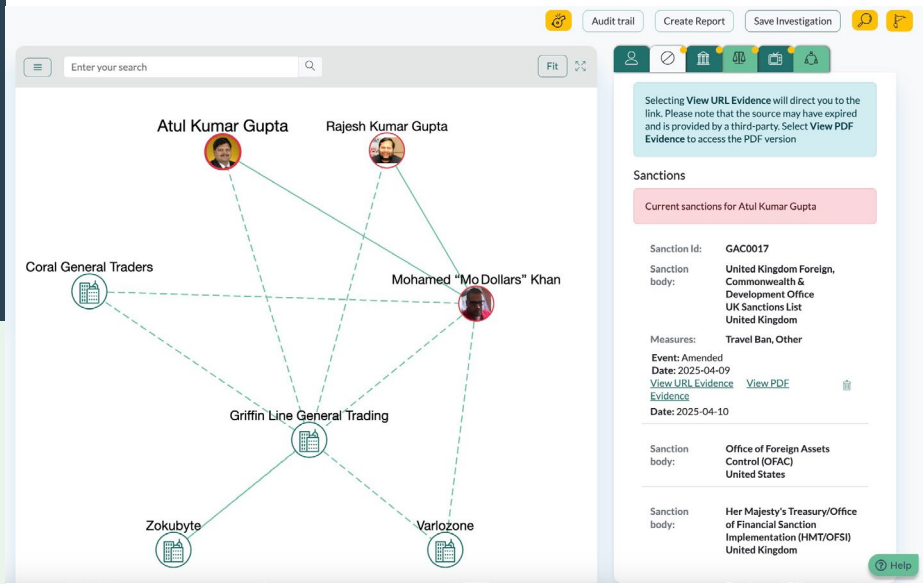
Two brothers from a prominent Indian business family, Atul and Rajesh Gupta, have faced years of allegations linking them to widespread corruption and financial misconduct. In 2022, they were arrested in connection with a far-reaching state capture scheme that allegedly enabled them to exert undue influence over South African government institutions. In total, the Guptas were able to reportedly secure at least $3.2 billion worth of government business through a vast network of corporations that obtained fraudulent contracts and used connections to get access to contracts in exchange for kickbacks. Central to their case is the use of front companies and layered banking structures spanning India, South Africa, the UAE, and Hong Kong—all used to move illicit funds, launder money, and secure state contracts through bribery and political manipulation.

Since the Gupta brothers' arrest, various connections to more crimes have come to light, including significant ties to the illicit gold trade in South Africa. Investigations by Al Jazeera and the Zondo Commission reported that a suspected money launderer, Mohamed "Mo Dollars" Khan, acted as a key facilitator for the Guptas. Khan, linked to gold-smuggling networks, reportedly controlled front companies—Varlozone, Zokubyte, and Coral General Traders—used to move Gupta-linked state funds offshore. These shell companies, in turn, reportedly sent large sums to Griffin Line General Trading in Dubai, owned by the Guptas. This illicit gold trade infrastructure—fake invoicing, bribed bank officials at Sasfin Bank, and merchanting schemes—was purportedly repurposed to launder tens of millions in funds generated from state capture.

KEY TAKEAWAYS:

- The Gupta case exposes gaps in India's corporate ownership disclosure, which can be exploited to hide illicit proceeds and obscure accountability in multinational corruption schemes.
- Criminal actors may exploit discrepancies between Indian financial regulations and those of other jurisdictions, using India as a conduit or safe haven for illicit flows tied to foreign corruption.
- The Gupta case serves as a cautionary example of how financial crime can intertwine with political patronage, necessitating vigilance around PEPs and political financing within India.
- The Gupta case demonstrates how environmental crime and resource contraband can be closely linked to political corruption and financial malfeasance.
- Indian financial institutions must enhance their KYC and transaction monitoring protocols, especially for clients with international exposure or ties to high-risk jurisdictions.

Why This Case Matters: Though the Gupta brothers built their corrupt empire largely in South Africa, their Indian origin and cross-border financial operations shine a spotlight on vulnerabilities in India's financial crime controls. The brothers used Indian financial systems, banks, and networks to move illicit funds and launder proceeds from their activities abroad. This exposes gaps in India's ability to monitor and regulate outward financial flows, beneficial ownership structures, and cross-border money laundering—especially when individuals operate across jurisdictions. Their case reveals how Indian nationals can become enablers or facilitators of corruption elsewhere while evading scrutiny at home.



Case Study

Maktab al-Siddiq

As part of the Islamic State's General Directorate of Provinces (GDP), the regional office Maktab al-Siddiq oversees IS finances across much of Asia. According to the US State Department, Maktab al-Siddiq employs unregistered money services businesses, established hawala networks, cash couriers, and virtual assets across South and Southeast Asia Afghanistan, Pakistan, India, Bangladesh, Maldives, and the Philippines. As a leading IS office, Maktab al-Siddiq generates revenue by transferring money from regional activities liked to extortion, kidnapping for ransom, and robbery. Leveraging these financial mechanisms, Maktab al-Siddiq supports a range of IS activities globally—including high-profile attacks, such as those carried out in Iran and Russia in recent years.

Why This Case Matters: The presence of Maktab al-Siddiq—a regional financial hub of the Islamic State—across South and Southeast Asia underscores a significant and persistent threat to India's financial integrity and national security. India's inclusion in this network highlights vulnerabilities in its informal financial systems, such as hawala, and raises concerns over terrorist financing risk exposure. The use of unregulated financial channels and virtual assets to fund extremist operations not only circumvents formal oversight but also exposes the Indian financial ecosystem to international scrutiny and reputational risk. As global terrorist networks decentralise and adapt to regional conditions, India's strategic location and high-volume cash economy make it a key transit and funding zone—necessitating stronger controls, intelligence coordination, and enforcement.

KEY TAKEAWAYS:

- Transnational terrorist and criminal networks operating across South and Southeast Asia expose financial institutions in India—as well as vulnerable sectors such as hawala operators and virtual asset providers—to elevated terrorist financing and predicate crime risks.
- The use of unregulated money services, hawala networks, cash couriers, and virtual assets by criminals—many of which remain outside the scope of India's formal financial regulatory frameworks—is a key risk in the country.
- The sourcing of funds through extortion, kidnapping for ransom, and robbery highlights the convergence between organised crime and terrorism financing.
- The use of India-linked financial channels increases the country's exposure to sanctions, FATF scrutiny, and international counter-terror financing enforcement.
- This case reinforces the need for institutions to strengthen internal awareness and enhance their CDD on high-risk jurisdictions and counterparties, especially those with links to terrorist organisations, conflict zones, or prevalent informal transfer systems.

Key Financial Crime Watchpoints

The following watchpoints highlight common financial crime risk indicators to look out for as regards clients, partners, suppliers, and broader business transactions and relationships. They are designed to support client risk assessments, enhanced due diligence and transaction monitoring by identifying patterns frequently associated with financial crime in India.

- **Complex ownership structures or the use of third-party intermediaries,** including multiple ownership layers or offshore entities, especially in jurisdictions with weak AML controls.
- **Financial or business connections** to high-risk regions within India (e.g. border areas with Nepal, Bangladesh, or the Northeast) known for trafficking or smuggling, terrorist financing, or informal trade.
- **High-risk sectors** prone to corruption or transnational crimes—such as infrastructure, mining, real estate, gems and jewelry, and other cash-intensive industries.

- **Corruption indicators** in businesses in public procurement and other government contracts, such as rapid revenue growth but limited operational footprint.
- **Counterparties in Russia, Iran, North Korea,** or third-party jurisdictions commonly used for sanctions evasion (e.g. Turkey, China).
- **Use of informal channels by clients or counterparties**, including hawala-based transfers (indicators may include, for example, offsetting cross-border transactions with no clear link or economic logic).
- **Unusual trade activity,** especially shipping routes through third countries or free trade zones (e.g. Dubai, Hong Kong) with no commercial reason.

How Themis Can Help

Financial crime has evolved faster than traditional systems. Themis delivers a new AI-powered, end-to-end platform purposebuilt to help businesses detect, prevent, and respond to threats in real time. A modular solution that fuses advanced analytics, automation, and proprietary intelligence to tackle risk at scale and fast. As financial crime becomes more complex, Themis delivers clarity, speed, and impact. This isn't an evolution. It's the platform the future demands — powered by data, powered by Themis.

Themis aims to be a leader in applying AI-led solutions to the problems of financial crime, and we are uniquely placed to do so. With strong working relationships with governments and businesses of many shapes and sizes, our software is developed with the needs of the whole financial crime compliance ecosystem in mind. By combining a focus on innovative technology with leading human intelligence and insight, Themis is capable of not only meeting those needs as they currently are but also anticipating them as they evolve in an uncertain future.

Our Reports and Services

Enjoyed this briefing? Keen for a more detailed analysis that's specific to your business? We deliver longer, bespoke reports and executive briefings about specific countries or sectors. Whether you're investing in new markets, expanding your own footprint or ensuring your financial crime country risk assessments align with the Wolfsberg Group's principles, our Risk Intelligence team can help. We specialise in complex, strategic projects where financial crime risks are new, emerging, or poorly understood.

Get in touch to find out more.

Our Team of Experts

Nadia O'Shaughnessy
Head of Insight
nos@wearethemis.com

Olivia Dakeyne
Principal, Research
od@wearethemis.com

Eliza Thompson
Financial Crime Researcher
et@wearethemis.com

Henry Wyard
Senior Policy Analyst
hjw@wearethemis.com

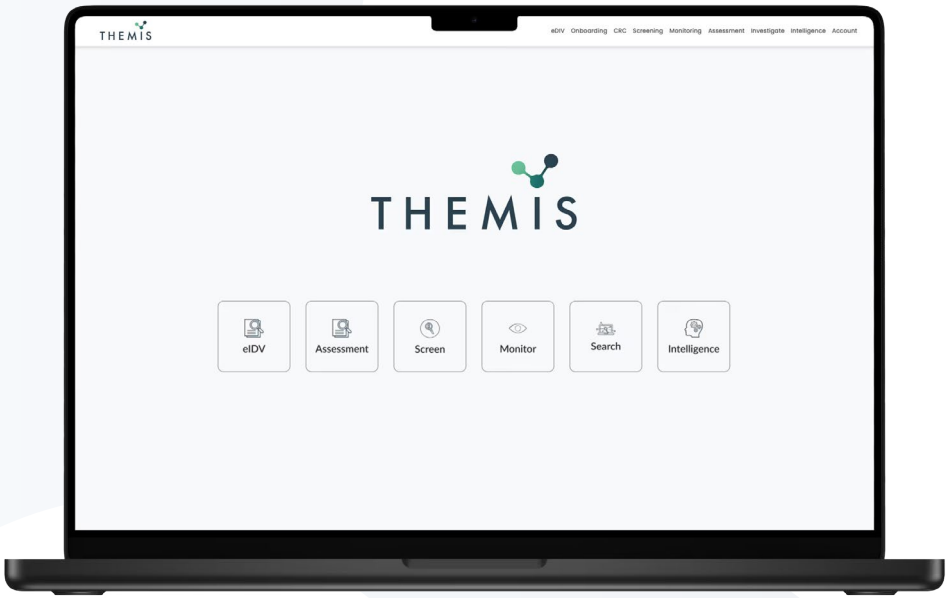
Nikhil Gandesha
Global Financial Crime Training Lead
ng@wearethemis.com

Emily Hsu
Financial and Environmental Crime Researcher
eh@wearethemis.com

Discover Other Country Risk Briefings

Research-driven analysis that informs and inspires action to tackle financial crime

Discover all



THEMIS

UK: +44 (0) 20 8064 1724 | UAE: +971 (0) 58 526 8765

info@wearethemis.com

www.wearethemis.com

Certified B Corporation