MINISTRY OF CORPORATE AFFAIRS
GOVERNMENT OF INDIA
Indian Institute of Corporate Affairs
Partners in Knowledge, Governance, Transformation
School of Finance and Management
विकसित भारत अभियान
1947 TO 2047

ECONOMIC SECURITY *Insights*

ISSUE 02
2026, April-June

INSIDE THE ISSUE

In a world of rising economic self-interest, the focus must be on strengthening India's capabilities, expanding opportunities, and empowering citizens.

SHRI NARENDRA MODI

HON'BLE PRIME MINISTER OF INDIA

INDIAN INSTITUTE OF CORPORATE AFFAIRS (IICA)

Indian Institute of Corporate Affairs (IICA) is established under the aegis of the Ministry of Corporate Affairs, Government of India, to be a think-tank for holistic advice on all issues relating to corporate affairs, including commercial dispute resolution. It is a think tank that curates a repository of data and knowledge for policy-makers, regulators, as well as other stakeholders working in the domain of Corporate Affairs. IICA carries out capacity building and training programmes, policy advisory functions, public outreach and stakeholder consultancy among various others.

SCHOOL OF FINANCE AND MANAGEMENT(SoFM)

School of Finance and Management is engaged in capacity building, education, research, advocacy and advisory on contemporary financial and regulatory issues, including banking, finance, financial reporting, economic crimes, leadership, valuation, risk management & allied themes.

It runs the flagship 12-Month Advanced Management Program in Corporate Affairs (AMP-CA). Another innovative 12-Month Masters in Financial and Economic Security (MFES) Program is run by the school as the first inter-ministerial collaborative initiative with Rashtriya Raksha University (RRU), Ministry of Home Affairs, Government of India.

The School has also curated programs like Financial Intelligence for Directors (FID), Risk Intelligence for Directors, Certificate Program for New Age Bureaucrats and Public Leaders, Advanced Finance for Finance Professionals (AFFP), Strategic Leadership Module and Certificate Program for Start-Ups. It also provides research, advocacy and advisory support to priority initiatives of the Government of India.

The School has so far trained 5000+ executives across board level, top management, middle management and entry level/induction through various online, in-person and hybrid programmes.

LEADERSHIP AT IICA

SMT. NIRMALA SITHARAMAN

HON'BLE UNION MINISTER OF FINANCE AND CORPORATE AFFAIRS

SHRI HARSH MALHOTRA

HON'BLE MINISTER OF STATE FOR CORPORATE AFFAIRS

DR. PALLAVI JAIN GOVIL

SECRETARY, MINISTRY OF CORPORATE AFFAIRS

SHRI GYANESHWAR KUMAR SINGH

DG & CEO

INDIAN INSTITUTE OF CORPORATE AFFAIRS

MESSAGE FROM DG & CEO

Dear Readers,

It gives me immense pleasure to present the second issue of Economic Security Insights, IICA's quarterly platform dedicated to examining the evolving dimensions of economic security and their implications for India and the global economy. Building upon the first issue, this edition continues our endeavour to facilitate informed dialogue and bring together diverse perspectives on developments shaping the economic security landscape.

The contours of economic security are changing rapidly. In an increasingly interconnected world, economic disruptions rarely remain confined to a single sector or geography. Geopolitical tensions, disruptions in critical supply chains, technological dependencies, cyber threats, illicit financial flows, and competition for strategic resources are increasingly interconnected. These developments underscore the need for a comprehensive understanding of economic security that extends beyond conventional economic indicators to encompass resilience, preparedness, institutional capacity, and strategic foresight.

For India, this evolving landscape presents both challenges and opportunities. As our economy expands and our global economic engagement deepens, strengthening the resilience of our financial systems, digital infrastructure, supply chains, critical sectors, and institutions becomes increasingly important. The vision of Viksit Bharat @2047 calls for not only sustained economic growth but also the ability to anticipate vulnerabilities, manage emerging risks, and safeguard the foundations of a resilient and secure economy.

This issue of Economic Security Insights brings together perspectives and analysis on developments relevant to economic security in India and globally. Through research, informed commentary, and diverse viewpoints, the newsletter seeks to promote greater awareness and encourage meaningful discussion on emerging challenges and opportunities. I hope the articles and insights featured in this edition will provide readers with valuable perspectives and stimulate further engagement with this important subject.

As IICA continues to strengthen its work in the area of economic security through knowledge creation, capacity building, and stakeholder engagement, I am confident that Economic Security Insights will grow into a meaningful platform for dialogue, knowledge-sharing, and informed debate. I invite our readers to engage with the publication and contribute to building a stronger body of knowledge around the economic security challenges of our time.

With best wishes,

Gyaneshwar Kumar

Gyaneshwar Kumar Singh
DG & CEO, IICA

सत्यमेव जयते

Indian Institute of Corporate Affairs

Partners in Knowledge. Governance. Transformation.

Azadi Ka Amrit Mahotsav

EDITOR'S NOTE

Dear Readers,

It is a pleasure to welcome you to the second issue of Economic Security Insights, covering the period April–June 2026.

The past few months have reinforced an important reality: economic security is no longer confined to financial regulation or conventional economic policy. Rapid technological change, sophisticated financial networks, cyber-enabled offences, illicit financial flows, and increasingly complex cross-border transactions are reshaping the nature of economic and financial crime. Addressing these challenges requires professionals who understand the interconnections between finance, law, technology, regulation, investigation, and national security.

At the Indian Institute of Corporate Affairs (IICA), our endeavour has been to contribute to this emerging ecosystem through knowledge, capacity building, and interdisciplinary engagement. Economic Security Insights is an extension of this endeavour, bringing together developments, perspectives, and analysis on issues that influence the resilience and security of economies and financial systems.

This issue examines contemporary developments in economic security in India and across the world. From financial crime and regulatory responses to technological developments and the evolving architecture of economic governance, the contributions seek to encourage informed discussion on the challenges confronting institutions in a rapidly changing environment.

A significant initiative in this direction is the Master's in Financial and Economic Security (MFES) programme, jointly offered by IICA and Rashtriya Raksha University (RRU). The programme brings together perspectives from economics, finance, law, technology, governance, and national security to develop specialised understanding of emerging economic and financial security challenges. Applications are now invited for the second batch of the MFES programme, and I encourage interested professionals and practitioners to explore this opportunity to strengthen their knowledge and capabilities in this field.

As Economic Security Insights enters its second issue, I hope it continues to serve as a platform for meaningful dialogue, critical thinking, and knowledge exchange. I warmly invite our readers to share their perspectives and contributions as we collectively deepen our understanding of economic security and its implications for India.

With best wishes,

Dr Naveen Sirohi

Prof (Dr) Naveen Sirohi
Head, School of Finance & Management
Course Director, Masters in Financial and Economic Security

Article

Economic Security in an Interconnected World: Why Financial Crime Prevention Matters for India

Mr. Michel Carles
Financial Crime Expert, UNDP
Former Anti-Fraud and Forensic Audit Expert, Organisation for Economic Co-operation and Development (OECD)

Executive Summary

Economic security has become one of the defining strategic imperatives of the mid-2020s. In an environment shaped by geopolitical fragmentation, digital acceleration, sanctions, illicit financial flows, and hybrid threats, the integrity of a country's financial system is no longer a technical compliance issue. It is a matter of national resilience, strategic autonomy, and global credibility.

For India, the stakes are particularly significant. The country is a rising economic power, a central actor in the Indo-Pacific, and a global leader in digital public infrastructure. Its financial system is expanding rapidly, supported by innovations such as UPI, Aadhaar, DigiLocker and India Stack. These assets have transformed financial inclusion and positioned India as one of the most dynamic digital economies in the world. Yet the same openness, speed and scale that underpin India's growth also create vulnerabilities.

Illicit financial flows now move across borders, platforms and jurisdictions with unprecedented speed. Criminal networks, corrupt actors, terrorist financiers, sanctions evaders and hostile state-linked actors exploit the same channels used by legitimate commerce: instant payments, cross-border trade, fintech platforms, crypto-assets, shell companies and global supply chains. Financial crime has therefore become systemic. It can erode tax revenues, distort markets, weaken institutions, undermine investor confidence and expose the country to geopolitical manipulation.

India's economic security over the coming decade will depend on its ability to prevent, detect and disrupt these flows. This requires more than regulatory compliance. It calls for an integrated national architecture combining financial intelligence, risk-based supervision, technology-enabled monitoring, beneficial ownership transparency, public-private partnerships and stronger cross-border cooperation.

This article examines the global economic security landscape, identifies the key financial crime risks facing India, draws lessons from high-performing jurisdictions, and proposes a strategic framework for strengthening India's resilience between 2026 and 2030.

1. Economic Security Has Become Financial Security

Economic security was once understood primarily through the lens of macroeconomic stability, industrial capacity, access to resources and protection of critical infrastructure. Today, that definition is no longer sufficient. In an interconnected financial system, a state's economic security also depends on its ability to protect the integrity of financial flows, prevent illicit finance, secure supply chains and withstand external manipulation.

The reason is clear: finance has become both an enabler of growth and a vector of vulnerability. Capital, trade payments, remittances, investments, digital transactions and crypto-assets circulate at high speed across borders. These flows support commerce and innovation, but they also provide channels for money laundering, terrorist financing, tax evasion, corruption, sanctions circumvention and cyber-enabled fraud. This transformation has shifted financial crime from the margins of economic governance to the centre of national strategy. A weak anti-money laundering and counter-terrorist financing framework can no longer be treated as a technical deficiency. It affects fiscal stability, market integrity, foreign investment, diplomatic credibility and national security. For emerging powers, this challenge is particularly acute. The more a country integrates into global markets, the more exposed it becomes to external financial risks. The more it digitizes, the faster both legitimate and illicit activity can scale. The more it participates in strategic trade corridors, the more it must manage exposure to trade-based money laundering, sanctions risk and supply-chain manipulation. India is therefore at a decisive moment. Its rise as a global economic power requires a corresponding strengthening of its financial integrity architecture.

2. The Global Context: Fragmentation, Digitization and Hybrid Threats

The period from 2024 to 2026 has been marked by three structural shifts that directly affect economic security.

Geoeconomic fragmentation

The global economy is increasingly shaped by strategic rivalry between major powers. The United States, China, the European Union and other major actors increasingly use economic instruments — sanctions, export controls, investment screening, technology restrictions and financial regulation — to pursue geopolitical objectives. This has created a less predictable operating environment for countries positioned between competing blocs. Finance is now an instrument of power projection. Sanctions can affect entities and jurisdictions far beyond the original conflict zone. Supply chains are being reorganized through "friend-shoring", "near-shoring" and strategic industrial policy. Trade corridors are being revalued not only for efficiency but for resilience and political alignment.

For India, this fragmentation creates both opportunity and exposure. As global companies diversify supply chains and seek alternatives to overconcentration, India can position itself as a strategic manufacturing, services and technology hub. But this role also increases exposure to sanctions spillovers, trade-based laundering, illicit procurement networks and geopolitical financial crime.

Full digitization of finance

The second structural shift is the digital transformation of finance. Instant payments, digital identity, embedded finance, fintech platforms, artificial intelligence and crypto-assets have dramatically increased the speed and scale of financial activity. India is one of the leading examples of this transformation. UPI has reshaped payments. Aadhaar has enabled large-scale digital identity. India Stack has created a foundation for digital public infrastructure with global significance. These developments have improved financial inclusion and efficiency. However, digital finance also changes the risk environment.

Criminal networks can use instant payments to fragment transactions, recruit digital money mules and launder funds through high-volume micro-transfers. Synthetic identities can be created using stolen or manipulated documents. Fraud can be automated. Crypto-assets can be used to move value across borders through offshore exchanges, decentralized platforms, stablecoins, mixers and privacy tools.

The challenge for India is not to slow innovation, but to secure it. Digital finance must be matched by digital financial crime prevention.

The rise of hybrid threats

The third major shift is the convergence of crime, geopolitics and statecraft. The distinction between criminal organizations, hostile state-linked actors, corrupt networks, terrorist financiers and shell-company structures is increasingly blurred. Financial crime can now serve broader strategic purposes: circumventing sanctions, financing influence operations, acquiring strategic assets, laundering corruption proceeds, disrupting markets or weakening institutions. In this context, illicit finance is not only an economic issue. It is a tool of hybrid pressure.

India's position in the Indo-Pacific, its proximity to sensitive trade corridors, its complex geopolitical balancing role and its expanding digital ecosystem make it a potential target for such hybrid threats. A strong financial intelligence and compliance framework is therefore essential to national resilience.

3. Why India is at the Centre of This Transformation

India's economic and technological rise places it at the centre of the global economic security debate. Several characteristics make India both strategically important and structurally exposed.

A rapidly expanding financial system

India's financial system has grown significantly in scale, complexity and digital sophistication. Banks, non-banking financial companies, payment aggregators, fintech firms, digital lenders, capital market intermediaries and insurance entities now form a broad and increasingly interconnected ecosystem. This creates opportunities for growth, inclusion and innovation. But it also creates supervisory complexity. Regulatory standards are not always uniform across sectors. Some entities, particularly in fintech, digital lending and non-bank finance, may operate with varying levels of oversight. These gaps create opportunities for regulatory arbitrage.

A financial system of India's scale requires risk-based supervision that can identify where vulnerabilities are most concentrated, rather than relying only on formal compliance checks.

A world-leading digital public infrastructure

India's digital public infrastructure is one of its greatest strategic assets. UPI, Aadhaar, DigiLocker and India Stack have demonstrated how digital systems can expand access, reduce friction and modernize public and financial services.

Yet scale creates exposure. High transaction volumes make it harder to detect illicit patterns without advanced analytics. Instant transfers reduce the time available for intervention. Identity-linked systems must be protected against synthetic identity fraud, compromised credentials and misuse. Digital channels can be exploited by cybercriminals, fraud networks and money mule operations. India has the opportunity to become a global leader in digital anti-money laundering and counter-terrorist financing. But this will require integrating artificial intelligence, network analysis, behavioural analytics and real-time risk scoring into the financial integrity ecosystem.

A large informal economy

India's formal economy coexists with a substantial informal sector. Cash-based transactions, informal value transfer systems, under-documented business activity and uneven compliance capacity remain important features of the economic landscape.

This does not simply create tax challenges. It also complicates anti-money laundering enforcement. Informality can provide entry points for illicit funds into the formal financial system, especially when combined with shell companies, trade mis-invoicing, hawala networks or informal lending. The transition from informality to formalization must therefore be viewed as part of India's economic security strategy.

Expanding trade corridors

India's growing trade links with the Middle East, ASEAN, Africa, Europe and the wider Indo-Pacific create major opportunities. But trade is also one of the principal channels for illicit financial flows. Trade-based money laundering can occur through over-invoicing, under-invoicing, false invoicing, misclassification of goods, use of shell import-export companies, phantom shipments and manipulation of trade finance. As India's trade volume grows, so does the need for integrated customs, banking, tax and corporate data analytics. Trade integrity is therefore central to India's fiscal security, supply-chain security and geopolitical autonomy.

4. India's Core Financial Crime Risks

India faces a broad set of financial crime risks that reflect its scale, diversity and international integration. Several typologies are particularly relevant.

Trade-based money laundering

Trade-based money laundering is one of the most significant risks for India. Its exposure derives from the size of its trade flows, the complexity of its supply chains, and the importance of corridors connecting India with the Middle East, Southeast Asia, Africa and Europe. Criminal networks can exploit gaps between customs data, banking records, shipping documentation and corporate ownership information. Mis-invoicing can be used to move value across borders while appearing to conduct legitimate trade. Shell companies can be created for import-export activity with limited commercial substance. Dual-use goods can be used to obscure procurement networks. A national trade-based money laundering prevention system should therefore be a strategic priority.

Digital mule networks and instant-payment abuse

UPI and other digital payment channels have enabled extraordinary gains in speed and access. But high-velocity payments can also be exploited by criminals. Digital mule networks use individuals or accounts to receive, split and transfer illicit proceeds rapidly, often through small transactions designed to evade detection. Traditional transaction monitoring systems were not designed for this scale and speed. India needs advanced behavioural analytics capable of identifying clusters, velocity anomalies, unusual transaction chains and coordinated mule activity.

Crypto-asset laundering

Crypto-assets have become a mainstream financial crime risk globally. They are used in ransomware, investment scams, sanctions evasion, terrorist financing, darknet markets, corruption laundering and offshore value transfer. India has taken steps to bring virtual digital assets within tax and reporting frameworks, but the regulatory architecture remains incomplete. Without comprehensive licensing of virtual asset service providers, full Travel Rule implementation, blockchain analytics and cooperation with offshore platforms, illicit actors will continue to exploit gaps. Crypto regulation should not be framed as a narrow market issue. It is part of India's financial integrity and national security agenda.

Synthetic identity fraud

Synthetic identity fraud combines real and fabricated identity elements to create false profiles that can be used to open accounts, obtain credit, commit fraud and launder funds. In a digital economy, this risk is amplified by stolen documents, compromised mobile numbers, AI-generated materials and weak onboarding processes. India's digital identity infrastructure provides a strong foundation, but it must be supported by robust verification, cross-checking and anomaly detection across Aadhaar, PAN, telecom KYC, banking records and fintech platforms.

Non-bank and fintech vulnerabilities

Non-banking financial companies, digital lenders, payment aggregators and fintech platforms play a crucial role in India's financial ecosystem. They support credit access, inclusion and innovation. However, uneven supervision, complex ownership structures, weak KYC controls, high transaction velocity and cross-border partnerships can create vulnerabilities. A harmonized AML/CFT rulebook across banks, NBFCs, fintechs, payment companies and virtual asset service providers would reduce regulatory arbitrage and strengthen system-wide integrity.

Trade-based money laundering controls

Countries that perform well against trade-based money laundering integrate customs, banking, tax, shipping and corporate ownership data. They use anomaly detection, price comparison tools, beneficial ownership checks and joint task forces involving customs, FIUs and law enforcement. India should develop a national trade-based money laundering analytics platform capable of identifying suspicious trade patterns, shell import-export companies and mis-invoicing schemes.

Risk-based supervision

International standards increasingly emphasize risk-based supervision. Regulators must allocate resources according to exposure, not merely institutional category. High-risk sectors, corridors, products and entities require more intensive oversight. For India, this approach is particularly relevant for NBFCs, digital lenders, payment aggregators, crypto-related entities, trade finance and high-risk geographic corridors. Risk-based supervision would allow regulators to focus attention where threats are most concentrated.

Corruption and beneficial ownership opacity

Opaque corporate structures remain a major enabler of illicit finance. Shell companies, nominee directors, layered ownership and offshore entities can be used to conceal corruption proceeds, procurement fraud, sanctions exposure and money laundering. India has made progress on beneficial ownership transparency, but further strengthening is needed. Beneficial ownership data must be accurate, verified, accessible to competent authorities, integrated into KYC processes and subject to meaningful penalties for false declarations.

5. Lessons from International Best Practice

High-performing jurisdictions offer important lessons for India. Their experience shows that effective financial crime prevention requires more than legislation. It requires institutional capacity, data integration, public-private cooperation and credible enforcement.

Strong and intelligence-driven financial intelligence units

In leading jurisdictions, the financial intelligence unit is not simply a recipient of suspicious transaction reports. It is an intelligence hub with analytical capacity, operational autonomy and the ability to coordinate across regulators, law enforcement and international partners. For India, this means strengthening FIU-IND's role as a central node in the economic security architecture. FIU-IND should have enhanced data access, advanced analytics, stronger cooperation with state-level agencies, and the capacity to provide high-quality typology guidance to reporting entities.

Crypto-asset regulation

Effective crypto oversight requires mandatory licensing for virtual asset service providers, Travel Rule implementation, blockchain analytics, strict KYC obligations, monitoring of mixers and privacy tools, and cooperation with foreign regulators. India should move toward a comprehensive crypto-asset regulatory framework that treats virtual asset service providers as part of the mainstream financial system.

Beneficial ownership transparency

Verified beneficial ownership registries are essential to combat money laundering, corruption and sanctions evasion. The most effective systems integrate ownership data with financial institutions, regulators and FIUs.

India should strengthen the accuracy and usability of its corporate ownership data, including through verification, penalties for false reporting and controlled access for competent users.

Public-private partnerships

Financial institutions, fintechs, payment companies, telecom operators and technology firms often detect risks before public authorities do. Public-private partnerships allow for faster sharing of typologies, indicators and threat intelligence. India should establish a national financial crime intelligence partnership bringing together public authorities and private-sector actors to address priority threats such as mule networks, crypto laundering, TBML and synthetic identity fraud.

Cross-border cooperation

Financial crime is transnational by design. Effective enforcement requires timely cooperation with foreign FIUs, regulators, law enforcement agencies and judicial authorities. Mutual legal assistance processes must be efficient, digital and operationally responsive. India should prioritize cooperation with jurisdictions central to its trade, remittance, investment and digital-finance corridors, including Singapore, the United Arab Emirates, ASEAN partners, the European Union, the United States and key African economies.

6. A Strategic Framework for India

India's response should be built around four mutually reinforcing pillars: institutional integration, regulatory modernization, technological leadership and geopolitical cooperation.

Pillar One: Institutional integration

India's economic security architecture should integrate financial intelligence, cyber risk, trade security, sanctions exposure and geopolitical analysis.

This could be achieved through a high-level national economic security coordination mechanism bringing together FIU-IND, the Reserve Bank of India, SEBI, IRDAI, the Ministry of Finance, the Ministry of Commerce, the Ministry of External Affairs, customs authorities, cyber agencies and law enforcement. The objective should not be to create additional bureaucracy, but to improve strategic coordination and ensure that financial threats are assessed as part of national security planning. FIU-IND should be further empowered as India's central financial intelligence hub, with enhanced analytical tools, stronger access to data and closer integration with state-level enforcement units.

Pillar Two: Regulatory modernization

India should move toward a unified, risk-based AML/CFT framework across the financial system. This would include harmonized KYC standards, common risk indicators, consistent enforcement principles and sector-specific guidance.

Priority areas include:

- enhanced supervision of NBFCs and digital lenders;
- licensing and oversight of fintechs and payment aggregators;
- comprehensive regulation of virtual asset service providers;

- stronger requirements for beneficial ownership disclosure;
- risk-based inspections for trade finance and high-risk corridors;
- stricter enforcement against repeated or systemic compliance failures.

Regulatory modernization should aim to reduce arbitrage between sectors and raise the baseline of integrity across the financial ecosystem.

Pillar Three: Technological leadership

India's digital infrastructure gives it a unique opportunity to lead globally in technology-enabled financial crime prevention. A national financial crime analytics capability could integrate data from banking, UPI, NBFCs, fintechs, trade finance, customs, GST, corporate registries and crypto analytics.

Artificial intelligence and network analysis could help detect mule networks, synthetic identities, unusual trade patterns, coordinated fraud, shell-company clusters and cross-border laundering. UPI analytics should become a priority area. India can develop models to identify velocity anomalies, micro-laundering, circular transfers and mule account clusters while preserving privacy and due process.

India should also develop a national synthetic identity detection system integrating identity, telecom and financial signals, subject to strong governance and safeguards.

Pillar Four: Geopolitical and cross-border cooperation

India's economic security strategy must be aligned with foreign policy. The country should deepen cooperation with partners that are central to its trade and financial corridors.

Priority areas include:

- TBML cooperation with the UAE, Singapore, ASEAN partners and African trade hubs;
- crypto-asset investigations with major regulatory centres;
- sanctions risk dialogue with the United States, the European Union and other partners;
- joint typology work with FATF-style regional bodies
- cross-border public-private partnerships on fintech and cyber-enabled financial crime.
- faster mutual legal assistance and asset recovery

By building trusted cooperation networks, India can better protect its financial system while strengthening its role as a responsible global economic actor.

7. Policy Priorities for 2026–2030

India's reform agenda should be sequenced in a pragmatic way.

Phase One: Foundations, 2026–2027

The immediate priority should be to establish the foundations of a modern economic security architecture. India should strengthen FIU-IND's autonomy and analytical capacity, launch a unified AML/CFT rulebook, begin comprehensive licensing of virtual asset service providers, improve NBFC supervision and deploy initial UPI analytics to detect mule networks. This phase should also include the creation of a national public-private partnership on financial crime, focused initially on digital fraud, payment abuse, crypto risks and trade-based laundering.

Phase Two: Integration, 2027–2028

The second phase should focus on data integration and operational coordination. India should launch a national TBML analytics platform integrating customs, GST, shipping, banking and corporate ownership data. Beneficial ownership verification should be strengthened and linked to KYC systems used by banks, NBFCs and fintechs. Synthetic identity detection should be scaled across the financial sector. State-level economic security units should be developed to support national intelligence and enforcement efforts.

Phase Three: Consolidation, 2028–2030

By the end of the decade, India should aim to operate a fully integrated, AI-enabled financial crime prevention ecosystem. This would include risk-based supervision across all major financial sectors, advanced monitoring of instant payments, comprehensive crypto oversight, verified beneficial ownership data, strong TBML controls and deep cross-border cooperation.

8. The Strategic Payoff for India

Strengthening financial crime prevention is not only about reducing illicit activity. It is a strategic investment in national power. A stronger financial integrity framework would generate several benefits.

- First, it would enhance investor confidence. Global investors increasingly assess governance, transparency, regulatory predictability and financial crime exposure when allocating capital. A robust AML/CFT system would reinforce India's attractiveness as an investment destination.
- Second, it would protect fiscal stability. Reducing illicit financial flows strengthens tax collection, reduces leakage and supports public investment.
- Third, it would improve market integrity. Stronger supervision reduces fraud, corruption and unfair competition, allowing legitimate businesses to operate on a more level playing field.
- Fourth, it would reinforce India's global leadership in digital governance. India has already demonstrated that digital public infrastructure can transform inclusion and service delivery. It can now demonstrate that the same infrastructure can support financial integrity, compliance innovation and economic resilience.

Conclusion: Economic Security as a Foundation of National Power

India's rise is one of the defining developments of the 21st century. Its demographic scale, technological capabilities, growth potential and geopolitical relevance position it as a central actor in the emerging global order. But in a world where finance, technology, trade and geopolitics are deeply interconnected, economic power must be protected by financial integrity. Illicit financial flows are not a peripheral risk. They are a strategic challenge. They can weaken institutions, distort markets, erode public trust and expose the country to external manipulation.

India has many of the necessary foundations: digital infrastructure, regulatory experience, a dynamic financial sector, international credibility and strategic ambition. The next step is integration. The country must connect its institutions, harmonize its regulations, leverage its data, deepen public-private cooperation and strengthen international partnerships. If India succeeds, it will not only protect its own economic security. It will help define a new global model for financial integrity in the digital age.

The world of 2026 is interconnected, contested and fast-moving. India's ability to thrive in this environment will depend on its capacity to secure the financial foundations of its growth.

India has the scale, the tools and the strategic vision. What remains is execution.

Disclaimer: *Views expressed are personal.*

The Convergence of Merger Control and Financial Crime Prevention: Rethinking India's Regulatory Architecture

Mr. Sarthak Dutta
Adv., Supreme Court of India,
BBA LL.B, LL.M (Criminal Law), Masters in Financial and Economic Security

Abstract

India's merger control framework under the Competition Act, 2002 has evolved significantly since the Competition Commission of India (CCI) began enforcing the law. While the regime effectively examines mergers for market concentration and consumer welfare, it continues to overlook the potential link between corporate mergers and economic crime. This article argues that merger review should move beyond traditional competition analysis to include forensic financial scrutiny, greater beneficial ownership transparency, and stronger inter-agency coordination not as a substitute for competition analysis, but as a narrow, risk-triggered addition to it. Drawing on Indian and international practice, the article distinguishes what current law requires from what the proposed reforms would add, and sets out a calibrated framework better suited to the realities of modern corporate India.

The Illusion of Separation: Competition Law and Economic Crime

When the IL&FS group collapsed in 2018, the shock came not from a merger review but from lenders and rating agencies discovering, years too late, that a systemically important infrastructure conglomerate had buried its debt inside more than 350 subsidiaries. DHFL's collapse followed a similar arc: a business that looked commercially sound to lenders and prospective acquirers until forensic auditors were finally let in. Neither failure was a merger-control failure in the narrow sense the CCI was never asked to bless either group's structure. But both illustrate exactly the kind of concealment a purely competition-focused merger review is not built to detect, and that could just as easily sit inside a transaction the CCI does clear. There remains a persistent institutional tendency to treat competition law and financial crime regulation as separate domains.

Competition authorities focus on market structure, pricing, and consumer welfare, while regulators such as the Enforcement Directorate (ED), the Serious Fraud Investigation Office (SFIO), the Securities and Exchange Board of India (SEBI), and the Financial Intelligence Unit-India (FIU-IND) investigate fraud, money laundering, insider trading, and securities violations within their own statutory mandates. That division is administratively convenient, but it no longer reflects how modern corporate transactions actually behave: mergers that substantially reduce competition and concentrate financial and decision-making power in a few dominant firms often create the very conditions - reduced competitive pressure, diminished external scrutiny, that enable fraud and market manipulation.

Recognising this relationship is not an attempt to expand competition law beyond its legitimate boundaries. It is an acknowledgement that a merger review indifferent to these governance risks risks overlooking consequences that extend well beyond competition itself.

There is also a quieter institutional reason this deserves attention now, distinct from any single scandal. India's competition and financial regulators were built in different decades, for different problems, by different ministries, and have never been asked to interoperate on a single transaction file. That absence of interoperability was tolerable when merger review was a narrower, more mechanical exercise. It is less tolerable in a market where a single combination can simultaneously raise questions of market share, beneficial ownership, and cross-border capital flow questions today answered by three different regulators who may never compare notes.

How Merger Control Works and Where It Stops

Sections 5 and 6 of the Competition Act, 2002 establish India's mandatory pre-merger notification regime: transactions exceeding prescribed asset and turnover thresholds must be notified to the CCI before implementation, which then assesses whether the combination is likely to cause an Appreciable Adverse Effect on Competition (AAEC) - weighing market concentration, entry barriers, countervailing buyer power, and the potential for coordinated conduct. Over the years, the CCI has built a mature jurisprudence: the horizontal-overlap analysis in CCI v. Thomas Cook (India) Ltd., the structural and behavioural remedies imposed in Sun Pharma-Ranbaxy, and the regional-dominance scrutiny in Holcim-Lafarge all demonstrate real sophistication in evaluating market effects.

In each of these matters, the Commission's inquiry ended once the competitive-effects question was answered; none involved any examination of the parties' financial disclosures, ownership chains, or the provenance of transaction funding, because none of that lay within its remit to examine.

The regime has also shown real capacity to modernise. The Competition (Amendment) Act, 2023, given effect through the CCI (Combinations) Regulations, 2024 notified in September 2024, introduced a deal value threshold (DVT) - transactions exceeding ₹2,000 crore now require CCI approval wherever the target has substantial business operations in India, regardless of asset or turnover size, and without the benefit of the de minimis exemption that previously shielded smaller-footprint deals. The change was designed to catch asset-light, data-rich digital acquisitions — including so-called "killer acquisitions" - that had escaped scrutiny under the older thresholds, and it was accompanied by a shorter review clock, cut from 210 to 150 days.

But the DVT, notably, is still a market-power proxy - a bigger net for the same kind of fish. It says nothing about who ultimately controls the acquiring entity, where acquisition funds originate, or whether the target's disclosed financials can be trusted. Under the current statutory framework, the CCI is neither required nor expressly empowered to examine the financial integrity of the parties, the legitimacy of acquisition funding, or the accuracy of financial disclosures.

That is not an oversight in the drafting; it reflects a coherent institutional design in which competition law and financial crime enforcement were kept deliberately separate. As transactions grow larger, more complex, and more financially sophisticated, that separation leaves a regulatory gap precisely where competition law and financial crime increasingly intersect.

It is worth being precise about how deliberate that separation is, because the reform proposed in Section VI has to work with it rather than against it. Nothing in the CCI's enabling statute prevents the Commission from asking a question about ownership or funding if a party volunteers the information; what the statute withholds is a mandate to require it, to verify it against independent records, or to treat an unsatisfactory answer as a ground for delaying approval. The gap, in other words, is not one of curiosity but of authority and authority is precisely what a legislative amendment, rather than administrative practice, is needed to supply.

The Anatomy of Economic Crime in Merger Transactions

Economic crime in mergers is neither peripheral nor speculative. It recurs across the transaction lifecycle from pre-deal valuation to post-merger integration - in patterns as sophisticated as the financial structures that enable them. What unites the four patterns below is not any single statutory failure but a structural one: each depends, for its success, on nobody with the authority to ask a hard question actually asking it before the deal closes. Competition analysis, by design, asks a different set of questions entirely about market share and substitutability, not about who is behind the money or whether the numbers in the data room can be trusted and so simply never encounters most of what follows.

Corporate Fraud and Valuation Manipulation

Acquisition targets have a structural incentive to present their financial condition favourably through aggressive revenue recognition, capitalised expenses that should have been written off, or contingent liabilities disclosed inadequately or not at all. India has already lived through the consequences, as the IL&FS and DHFL episodes described above make clear: in both cases, corporate complexity actively impeded detection until it was too late for anyone but forensic auditors to intervene. Neither episode was uncovered by a market-share test, because a market-share test was never designed to look for it. A merger review indifferent to financial statement integrity has no mechanism for catching this before, rather than after, approval which is precisely when catching it would matter, both to the acquirer inheriting the liability and to the market absorbing the shock once it surfaces.

Insider Trading and Information Asymmetry

Merger negotiations are among the most significant sources of price-sensitive information in securities markets, extending over months and drawing in bankers, lawyers, auditors, and senior executives who all gain access to material non-public information. The Satyam Computer Services scandal, though primarily an accounting fraud, also showed how weak corporate governance and concentrated managerial control create opportunities for securities market misconduct. SEBI's Prohibition of Insider Trading Regulations, 2015 impose trading-window restrictions and disclosure obligations, but the framework remains substantially reactive — it punishes leakage after the fact rather than testing, at the point of merger review, whether the parties' information controls were adequate to prevent it in the first place.

A merger review that asked even a single question about information-governance controls during the notification stage would shift some of this burden from enforcement to prevention, complementing rather than duplicating SEBI's existing regime.

Money Laundering through Acquisition Structures

Complex cross-border mergers often involve layered holding companies, special purpose vehicles, and multi-jurisdictional financing that, while frequently legitimate, can also conceal the true source of funds or the identity of ultimate controllers. India's own regulatory record supplies a more precise data point than is often cited in this debate: in its 2024 mutual evaluation, the Financial Action Task Force placed India in its highest compliance category - "regular follow-up" a status only a handful of G20 economies hold, and credited the country with strong results on financial-intelligence use and international cooperation. Yet the same evaluators flagged a specific weakness: verifying beneficial ownership becomes markedly harder wherever control is exercised through indirect means or complex structures, a gap supervisory inspections had already surfaced within regulated financial institutions.

If beneficial-ownership verification is already strained in routine financial supervision where institutions have compliance teams built for exactly this purpose it is unlikely to be reliably self-policed inside a merger a corporate group has every commercial incentive to close quickly and quietly.

Bid-Rigging in Public Sector and Infrastructure Divestments

India's disinvestment programme and infrastructure sector frequently involve high-value acquisitions through competitive bidding, which are susceptible to bid-rigging parties that appear to compete secretly coordinating their bids. The relationship to mergers is structural, not incidental: as consolidation reduces the number of independent bidders, the likelihood of coordination among those remaining may increase. A merger that removes a significant competitor from future public procurement can, without any single anti-competitive act occurring at the time of approval, weaken competitive bidding years later an effect a static, point-in-time AAEC test is not designed to capture, because the harm it should be watching or has not yet occurred and may never be traceable back to the merger that enabled it.

Merger review should therefore weigh not only immediate concentration effects but whether a proposed combination is likely to diminish competition in future government procurement markets.

The Digital Economy Dimension

The digital economy has altered the relationship between mergers, competition law, and economic crime. Digital platforms derive advantage not only from scale but from the data they control, and "killer acquisitions", where dominant firms acquire innovative start-ups before they mature into competitors can suppress future innovation rather than merely reducing existing competition. Such acquisitions do more than shrink current market shares; they can eliminate the very firms capable of challenging established leaders, so the competitive harm extends beyond present-day metrics into the market's long-term evolution. The CCI's 2020 e-commerce market study and subsequent platform investigations reflect a growing institutional awareness of this risk, and the DVT was partly a legislative response to it, since asset-light digital targets had previously escaped scrutiny altogether.

It is worth noting, however, that the empirical case for describing killer acquisitions as widespread in Indian markets remains thin, and startup deal activity has in any case fallen sharply amid the recent funding slowdown. Reform proposals in this space should therefore be calibrated to genuine, observable risk indicators opaque financing, undisclosed control, a history of regulatory evasion rather than to a blanket presumption that consolidation itself is the harm. Algorithmic pricing adds a further complication: competing firms deploying similar pricing algorithms can produce outcomes resembling cartel behaviour even without direct communication, making the line between lawful parallel conduct and unlawful collusion progressively harder to draw as digital mergers accelerate the adoption of algorithm-driven strategies.

Comparative Perspectives: What Other Jurisdictions Have Done

India's regulatory challenge is not unique. Several jurisdictions have recognised that merger review cannot be confined to competition concerns alone, and have built mechanisms that integrate broader governance and financial-integrity considerations into transaction oversight without folding those considerations into competition law itself. In the European Union, merger control operates alongside a distinct anti-money laundering framework requiring enhanced due diligence for high-risk entities, and the proposed Corporate Sustainability Due Diligence Directive extends corporate due diligence into governance and human-rights risk.

The United Kingdom has gone further toward formal integration: the National Security and Investment Act 2021 created a standalone review mechanism for transactions posing national security risk, running in parallel with the Competition and Markets Authority's merger jurisdiction, while the Serious Fraud Office has, in overlapping cases, coordinated with competition enforcers where cartel conduct and financial fraud converged. In the United States, the Department of Justice and Federal Trade Commission have, in selected matters, coordinated with the Securities and Exchange Commission and the Financial Crimes Enforcement Network where a merger raised concerns beyond competition.

India already possesses comparable institutional building blocks - the CCI, SEBI, the ED, FIU-IND, and the SFIO each hold intelligence relevant to different aspects of corporate conduct but, unlike its counterparts abroad, has no formal protocol for routing that intelligence into a merger file. The comparative lesson is not that India should import any single foreign model wholesale, but that in every jurisdiction surveyed here, the competition regulator remains a consumer of financial-crime intelligence generated elsewhere, never its producer, and none is asked to develop forensic-accounting or anti-money-laundering expertise in-house. That design choice, more than any specific mechanism, is the one India's own reforms should borrow first.

The Case for Structural Reform

The convergence of competition law and economic crime prevention is not a future aspiration; it is a present necessity. Each reform below is framed against what current law requires, so the distance between the status quo and the change being urged is explicit rather than implied, and each is deliberately risk-triggered, so that routine combinations continue to clear exactly as they do today. The five proposals are also sequenced deliberately.

The first two- forensic due diligence and beneficial ownership verification generate the information the CCI presently lacks. The third - inter-agency coordination, ensures that information, once generated, reaches the regulators positioned to act on it. The fourth- post-merger monitoring recognises that integrity risk does not end at the approval order. And the fifth, the AAEC amendment; supplies the statutory authority without which the first four would sit outside the CCI's mandate altogether, however sensible they might be as administrative practice.

Mandatory Forensic Due Diligence for Significant Transactions

Current law requires no independent forensic financial report as part of merger notification; the CCI's inquiry is confined to competitive effects. Large transactions particularly those exceeding the DVT or involving strategically important sectors such as banking, financial services, infrastructure, or digital platforms should instead be accompanied by an independent forensic financial report, prepared by a qualified forensic accountant and reviewed by the CCI in consultation with the SFIO or FIU-IND where the report itself surfaces a red flag. The precedent is close at hand: India's Insolvency and Bankruptcy Code already relies on independent valuations and, where necessary, forensic audits during resolution.

Beneficial Ownership Disclosure as a Pre-Condition for Approval

Currently, the Competition Act does not require disclosure of ultimate beneficial ownership as a condition of approval, and the CCI has no mandate to verify ownership claims against the Ministry of Corporate Affairs, SEBI, or foreign registry records. Every party to a notifiable merger should instead be required to disclose ultimate beneficial ownership up to the natural person exercising control, verified against those records. Given the FATF's own finding that beneficial-ownership verification weakens precisely where control is layered or indirect, approval should remain pending not automatically refused wherever ownership cannot be established with reasonable certainty, with referral to FIU-IND reserved for opaque or high-risk structures rather than applied as a default. Greater transparency here would make it harder to conceal illicit ownership or the source of acquisition funds without adding friction to transactions with nothing to hide.

A third, quieter objection deserves acknowledgement: that added scrutiny, however narrowly targeted, will still be read by the market as added risk, with a chilling effect on cross-border investment into India at a time when attracting that investment is a policy priority in its own right.

This is a real trade-off, not an imagined one, and the risk-based design proposed here is the answer to it rather than a way of avoiding the question: a transaction with clean ownership, transparent financing, and no history of regulatory evasion should clear no more slowly under this framework than it does today. The added friction falls, by design, only on the transactions that would otherwise pass through unexamined.

Institutionalized Inter-Agency Coordination

No statute today requires or enables SEBI, the ED, SFIO, FIU-IND, or the RBI to share investigation-relevant intelligence with the CCI during merger review; each regulator's information remains, by default, within its own silo. India should instead establish a formal coordination mechanism drawing on the joint working-group models already used in cybersecurity governance, enabling timely sharing of information material to a proposed merger, including ongoing investigations and financial intelligence.
Such a framework would not diminish any regulator's statutory independence or require unrestricted disclosure of confidential information; it would simply ensure that intelligence one regulator already holds is not systematically invisible to another making a decision that intelligence would inform.

Post-Merger Monitoring and Compliance Frameworks

At present, the CCI's post-merger oversight is confined to verifying compliance with structural or behavioural remedies already imposed as conditions of approval; it has no general power to revisit an approval on integrity grounds once granted. A more comprehensive framework should require periodic reporting on governance and continued compliance with the representations made during review, coupled with clear statutory authority for the CCI to refer material deviations particularly evidence of concealment or fraudulent disclosure to the appropriate financial crime agency. In exceptional cases where approval itself was procured through fraud, the CCI should also have the power to seek proportionate remedies, including unwinding the transaction, so that approval marks the beginning of an ongoing obligation rather than the end of regulatory oversight.

Strengthening the AAEC Framework to Include Economic Crime Risk

Section 20 of the Competition Act defines the factors relevant to an AAEC assessment today, and financial integrity risk is not among them so the CCI has, quite properly, no locus to act on such a concern even where the four reforms above have already surfaced one. A more enduring solution would amend the Act to recognize financial integrity and economic crime risk as a relevant, though subordinate, consideration within the AAEC assessment: not a parallel test, and not a substitute for competition analysis, but an evidentiary input the CCI may draw on where warranted. This keeps competition analysis as the Commission's central, unaltered mandate while giving it an explicit statutory basis to act on integrity concerns it would otherwise have no authority to consider.

Objections and Their Limits

Supporters of the existing framework raise a legitimate concern: that broadening the CCI's mandate could produce regulatory overreach, discourage legitimate mergers, and duplicate the work of agencies better equipped to investigate financial crime. This objection has genuine force, but it is answerable by design rather than by dismissal. Every proposal above is deliberately risk-triggered, not universal modelled on the enhanced due diligence approach already used in anti-money laundering regulation, where additional scrutiny attaches only to transactions exhibiting identifiable risk factors: complex ownership, opaque financing, offshore structuring, or a documented history of regulatory non-compliance. Routine combinations, which make up the overwhelming majority of CCI filings, would proceed exactly as they do today, on exactly the current timeline.

The duplication concern rests on a narrower misconception. None of these proposals asks the CCI to conduct forensic audits or criminal investigations of its own; those responsibilities remain, undisturbed, with the ED, SFIO, SEBI, and FIU-IND.

What is proposed is that the CCI's own assessment be informed by intelligence those agencies already hold coordination, not expansion, of statutory function. A regulator that can already block a transaction outright on competition grounds is not being asked to acquire new coercive powers; it is being asked to see a fuller picture before it exercises the powers it already has.

A third, quieter objection deserves acknowledgment: that added scrutiny, however narrowly targeted, will still be read by the market as added risk, with a chilling effect on cross-border investment into India at a time when attracting that investment is a policy priority in its own right. This is a real trade-off, not an imagined one, and the risk-based design proposed here is the answer to it rather than a way of avoiding the question: a transaction with clean ownership, transparent financing, and no history of regulatory evasion should clear no more slowly under this framework than it does today. The added friction falls, by design, only on the transactions that would otherwise pass through unexamined.

Conclusion: Competition Law as a Bulwark Against Economic Crime

India stands at an important juncture in the evolution of its economic governance. As corporate consolidation accelerates, digital markets concentrate further, and financial transactions grow more sophisticated, a merger control regime built exclusively for market analysis is being asked to govern an economy where ownership structures are more layered and cross-border financing more opaque than the regime was designed to see.

The five reforms proposed here risk-triggered forensic review, verified beneficial ownership, formal inter-agency coordination, post-merger monitoring with a conditional unwinding power, and a modest statutory hook within Section 20 are calibrated to avoid the overreach their critics rightly worry about, while closing a gap India's own regulatory record shows is real. None of it asks the Competition Commission of India to become a financial crime regulator, and none of it requires an unfamiliar philosophy of regulation: each proposal extends a technique Indian law already uses elsewhere forensic valuation under the IBC, enhanced due diligence under AML law, joint working groups in cybersecurity into a merger control regime that has, until now, remained a closed loop.

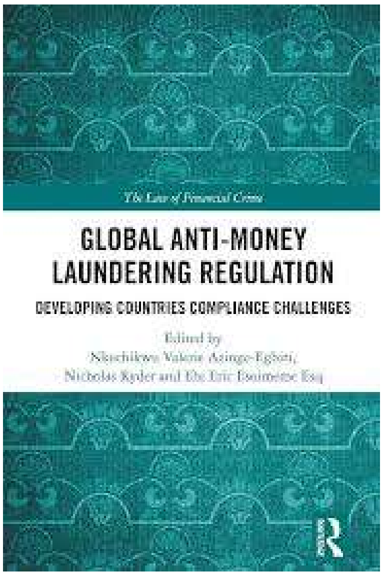
None of this requires India to wait for a crisis to legislate. The building blocks the IBC's forensic-audit practice, the FATF's own beneficial-ownership findings, the DVT's proof that Parliament will widen CCI jurisdiction when the case is made, and comparable coordination models already running in the EU, the UK, and the US already exist. What is missing is the decision to connect them inside a single transaction file, at the point where connecting them would actually matter: before approval, not after collapse.

The next concealment of the kind that took down IL&FS and DHFL need not be discovered only after the fact, by lenders and rating agencies working backward from a collapse. If it is travelling inside a transaction the CCI is already reviewing for its effect on competition, a modestly widened, carefully bounded merger review is positioned to see it first not instead of India's financial crime regulators, but alongside them. Effective competition enforcement and robust financial crime prevention are not competing priorities; they are complementary pillars of a well-regulated and trustworthy market economy.

Disclaimer: *The author practices at the intersection of competition law and regulatory compliance. Views expressed are personal.*

Book Review

Beyond the FATF Blueprint: A Review of Global Anti-Money Laundering Regulation: Developing Countries Compliance Challenges



Prof (Dr) Naveen Sirohi
Head, School of Finance & Management, IICA
Course Director, Masters in Financial and Economic Security

Mr. Abbas
Chief Programme Executive, Center Regulatory Governance, IICA
Course Coordinator, Foundational Course On Regulatory Governance

Abstract

For thirty years the Financial Action Task Force has set the terms on which the world fights money laundering and terrorist financing, and for nearly as long the burden of meeting those terms has fallen heaviest on countries that had no seat at the table when the standards were written. This edited collection, gathering fifteen chapters from scholars and practitioners working across Africa and the Small Island States, sets out to correct a literature that has looked mostly at London, Washington and Brussels while the majority of the world's national AML/CFT systems now sit in the developing world. The volume moves from the architecture of FATF listing and greylisting through country-level studies of Nigeria, South Africa and Botswana to cross-cutting chapters on politically exposed persons, beneficial ownership and asset recovery in states with thin institutional capacity. Its central argument is not that developing countries resist compliance out of indifference, but that a one-size-fits-all regime, designed around G7 banking systems, generates its own unintended consequences when transplanted elsewhere. The book succeeds as a corrective and a reference point, even where its country coverage tilts heavily toward Anglophone Africa and its individual chapters vary in analytical depth. It is a genuinely useful, well-documented addition to the financial crime literature and a timely one for any jurisdiction still negotiating its place within the FATF system.

Keywords: anti-money laundering, FATF, counter-terrorist financing, developing countries, financial crime regulation, beneficial ownership, blacklisting, Global South compliance

The Regulatory Problem: One Standard, Uneven Ground

The Financial Action Task Force occupies an odd position in the landscape of international regulation. It is not a treaty body, has no binding legal force of its own, and yet its forty recommendations have become the de facto global law of money laundering and terrorist financing, enforced through peer-reviewed mutual evaluations and the constant threat of being named to its grey or black lists. Azinge-Egbiri, Ryder and Esoimeme open their collection with a simple but pointed observation: these standards were built around the banking systems, judicial capacities and administrative resources of the G7, then extended to every jurisdiction regardless of its actual exposure to laundering or terrorist-financing risk, or its absence from the room where the standards were drafted. That asymmetry is the book's organising problem, and the editors are careful not to reduce it to a simple story of Northern imposition and Southern resistance

Developing states, the introduction argues, have in fact worked hard to demonstrate compliance, often at real cost to sovereignty and administrative bandwidth, precisely because the reputational and financial consequences of grey-listing (de-risking by correspondent banks, capital flight, diminished access to international finance) fall disproportionately on economies that can least absorb them. What the volume sets out to show, chapter by chapter, is how that compliance actually unfolds on the ground: which parts of the FATF template travel well, which produce unintended harm, and where the gap between formal adoption and substantive implementation is widest.

This is well-trodden ground in the abstract, but the empirical gap the editors identify is real. Existing scholarship on AML/CFT, as the introduction notes, remains heavily weighted toward the experience of the developed economies that designed the regime, even though the majority of countries now subject to FATF-style evaluation are outside that group. A collection built specifically around African states and Small Island Developing States is, on that basis alone, filling a documented hole in the literature rather than restating what is already well covered elsewhere.

The Editors and Their Project

The three editors bring complementary vantage points to the project. Nicholas Ryder, Professor in Financial Crime at Cardiff University's School of Law and Politics, is among the more prolific voices in UK financial crime scholarship, with a body of work spanning counter-terrorist financing law, financial crisis regulation and white-collar crime; his presence anchors the volume's engagement with the FATF architecture as it is understood in the jurisdictions that built it. Nkechikwu Valerie Azinge-Egbiri, Lecturer in Business and Commercial Law at Lancaster University and previously at the University of Lincoln, works specifically on the relationship between global financial crime regulation and economic development, and on the AML/CFT compliance trajectories of emerging economies -- a research interest that gives the volume its Global South orientation rather than treating it as an afterthought to a Northern template.

Ehi Eric Esoimeme, the third editor, supplies the practitioner's depth: a Professor of Business Law and Ethics with concurrent academic appointments in Nigeria, Liberia and the United States, and the author of more than a dozen books on financial crime compliance, one of which was independently ranked among the field's most influential money-laundering titles. That combination -- a UK-based comparativist, a scholar of financial crime and development, and a widely published West African practitioner-academic -- is precisely what the subject demands, and it shows in the book's willingness to let African contributors write from direct professional experience of the compliance burdens they describe, rather than filtering the material entirely through outside observation.

Structure and Organisation

The volume runs to fifteen chapters across 332 pages, opening with a foreword from Sope Williams and an editors' introduction that lays out the book's argument and its organising logic. The chapters then move outward in three broad movements, though the book does not label them as such. The first cluster works at the level of the FATF system itself: the politics of standard-setting, the ambiguities in how the international regime treats African states as a bloc, and the mechanics and consequences of blacklisting and greylisting, including a chapter co-authored with Donato Masciandaro, whose earlier work on the political economy of financial regulation is well known in the field.

A second cluster narrows to country case studies -- South Africa's experience with banks unilaterally terminating customer accounts under AML pressure, Botswana's legal culture and its effect on AML/CFT prosecution, and several Nigeria-focused chapters covering barriers to adopting new compliance technologies, the specific difficulties financial institutions face in meeting AML obligations, and the laundering risks posed by politically exposed persons.

West Africa's regional FATF-style body, GIABA, gets its own chapter, which is a sensible inclusion given how much of the country-level material that follows sits within GIABA's mutual evaluation framework.

The third movement pulls back out to cross-cutting themes that cut across the country material: the vulnerability created by weak beneficial ownership transparency, whether FATF's beneficial ownership push actually helps anti-corruption work in low-capacity settings, the particular difficulty of countering terrorist financing where state capacity is already stretched, and a chapter on asset recovery co-authored by Jean Pierre Brun, whose background at the World Bank's Stolen Asset Recovery Initiative lends real institutional weight to that discussion. The book closes with a chapter on strategic tools for improving AML/CFT compliance, functioning as something close to a policy conclusion rather than a conventional summary chapter.

The Politics of Listing: Who Judges Compliance, and On What Terms

The strongest material in the book's opening section is also its most conceptually ambitious. Constance Gikonyo's chapter on the ambiguities within the international AML regime as it applies to African states is a genuinely useful corrective to the tendency, visible in much FATF-adjacent commentary, to treat African compliance failures as a monolithic story of capacity shortfall. Gikonyo instead traces specific conflicts in how the standards are interpreted and applied, showing that non-compliance is frequently a product of contradictory guidance rather than simple unwillingness or incapacity. The blacklisting chapter, co-written by Azinge-Egbiri with Joy Malala and Donato Masciandaro, is where the book's central argument sharpens into something closer to a testable claim: that FATF listing decisions function less as a neutral technical assessment and more as a reputational instrument whose consequences are severe and whose criteria are not applied with full consistency. This is not a new observation in the wider financial crime literature, but the chapter grounds it specifically in African cases, which is where the collection's contribution lies. Readers looking for a rigorous statistical test of listing consistency across regions will not find one here; the chapter is closer to a structured argument supported by case evidence than an econometric study, and it reads as such.

Implementation on the Ground: Banks, PEPs, and the Limits of Formal Compliance

The country-level chapters are where the volume earns its keep as an empirical resource rather than a restatement of familiar critique. Zakhele Hlophe's account of South African banks unilaterally closing customer accounts to manage AML risk a practice with obvious parallels to correspondent-banking de-risking discussed in the broader financial inclusion literature shows how AML compliance, pursued defensively by financial institutions rather than in coordination with regulators, can end up excluding legitimate customers rather than catching illicit ones. It is a sharp illustration of the book's larger point: formal adherence to FATF norms does not guarantee that the underlying policy goal is actually served.

The Nigeria-focused chapters, several of them, form the thickest part of the collection, which is both a strength and a limitation worth naming plainly. Esoimeme's own chapter on barriers to adopting new AML/CFT technologies is grounded in direct practitioner familiarity with Nigerian financial institutions and is candid about where technological solutions are oversold relative to what under-resourced compliance functions can actually operate. The chapters on politically exposed persons Chinelo Bob-Osamor on the specific vulnerability created by PEP laundering in Nigeria, and John Hatchard's continental treatment of PEP exposure and beneficial ownership transparency work well in sequence, moving from a single-country problem to the broader institutional question of whether beneficial ownership registers, FATF's preferred remedy, can function at all where corporate registries themselves are unreliable. Jackie Harvey and co-authors push that scepticism further, asking directly whether FATF's beneficial ownership focus actually helps anti-corruption work in 'low-capacity' states or whether it adds a compliance burden without a matching enforcement gain one of the more analytically honest chapters in the book, willing to answer its own question in qualified rather than celebratory terms.

Terrorist Financing and Asset Recovery Under Capacity Constraints

Simeon Igbinedion's chapter asks, in its title, whether developing countries can win the fight against terrorist financing at all under current resourcing, and answers with careful pessimism rather than either alarmism or false reassurance -- a register the book's better chapters share throughout. Dominic Thomas-James turns to the Small Island States, examining the willingness of small jurisdictions to comply with suspect-wealth rules when their financial sectors are, in relative terms, disproportionately exposed to the reputational consequences of any single high-profile case. This chapter is one of the few in the collection to move outside the African case studies, and the book would have benefited from more material at this scale, since the Small Island States promised in the subtitle receive comparatively thin treatment set against the depth given to West and Southern Africa.

The asset recovery chapter, co-authored by Jean Pierre Brun and Anastasia Sotiropoulou, is one of the collection's most technically assured contributions, tracing why recovered assets so rarely make their way back to the jurisdictions from which they were stolen and what procedural and jurisdictional obstacles stand in the way. It functions almost as a stand-alone primer on asset recovery mechanics and would be useful reading on its own, independent of the volume's wider argument about FATF transplantation.

Critical Assessment: Contributions, Limitations, and Unanswered Questions

The book's central contribution is straightforward to state and genuinely earned: it assembles, in one place, empirical and doctrinal material on AML/CFT compliance in states that the mainstream financial crime literature has largely treated as case notes rather than as the primary subject of analysis. The endorsements from Jason Sharman, whose own work on the political economy of global AML standards is a touchstone in the field, and from Etannibi Alemika, a veteran scholar of criminology in the region under study, are not throwaway jacket copy; both point specifically to the scarcity of prior academic literature on the issues the book covers, and that scarcity is real. For researchers, compliance officers or regulators trying to understand how FATF standards actually function once they leave Paris, this is a rare single-volume resource.

Its limitations follow fairly directly from its strength. The geographic promise of the subtitle -- developing countries broadly -- is not quite matched by the geographic reality of the contents, which lean heavily toward Anglophone West and Southern Africa, with Nigeria in particular carrying a disproportionate share of the country-level chapters. Latin America and South and Southeast Asia, regions that between them contain a large share of the world's developing-country FATF membership and its own history of grey-listing episodes, are absent entirely.

The Small Island States named in the subtitle receive one dedicated chapter against roughly a dozen chapters weighted toward the African continent, which reads as an imbalance the editors could have addressed either by adjusting the subtitle or by commissioning additional material.

As with most edited collections assembled from a wide range of contributors, the chapters vary in analytical ambition. Some, like the beneficial ownership and blacklisting chapters, build genuine arguments and engage critically with the FATF's own assumptions; others read closer to descriptive compliance surveys, useful as reference material but offering less by way of independent analytical contribution.

The book also does not attempt a systematic comparative framework across its fifteen chapters -- no concluding chapter draws the country case studies into a single comparative table or typology of compliance pathways, so the reader is left to do that synthesising work independently. Given the editors' own argument that comparative, cross-regional understanding is exactly what the literature lacks, a more deliberate comparative apparatus would have strengthened the volume's claim to closing that gap rather than simply gathering material adjacent to it.

Conclusion: Relevance for Regulators Beyond Africa

None of these limitations diminish the book's core value, which lies less in any single chapter than in the cumulative weight of fifteen accounts converging on the same structural point: a compliance regime built around the institutional assumptions of the wealthiest economies will behave differently, and sometimes counterproductively, when applied elsewhere without adjustment for local capacity, legal culture and financial-sector structure. That argument travels well beyond the African and Caribbean contexts the book examines directly. Regulators in India and other large developing economies navigating their own FATF mutual evaluations, beneficial-ownership reforms under the Prevention of Money Laundering Act framework, and the perennial tension between capacity-building and formal rule adoption will recognise almost every dynamic this book describes, even where the country names differ.

For the Centre for Regulatory Governance's own community of regulators, researchers and policy practitioners, the book's real utility is as a comparative mirror: a detailed account of how a comparable set of compliance pressures has played out elsewhere in the Global South, complete with the specific mechanisms -- defensive de-risking by banks, PEP exposure in weak beneficial-ownership systems, capacity-constrained counter-terrorist-financing regimes -- that Indian regulators are likely to encounter in some form of their own. It is not a comprehensive global survey, and readers seeking Asian or Latin American case material will need to look elsewhere to complete the picture. But as a well-documented, critically engaged study of how the FATF system actually functions once it leaves the jurisdictions that designed it, this collection is a valuable and recommended addition to the financial crime and regulatory governance shelf.

Disclaimer: *The reviewer declares no financial or personal relationship with the author or publisher of the work under review.*

Indian News and Trends

Energy self-reliance: Next pillar of India's economic security

The ongoing conflict in the Gulf and its impact on global energy are a powerful reminder of why energy self-reliance is crucial for every nation. The war has entered its third week with no clear end in sight, and its repercussions are being felt across the globe, with spiking energy prices due to the disruption of oil and gas supplies. LPG and LNG prices have already spiked in India. Petrol and diesel remain stable for now. In tier-2 and tier-3 cities, domestic and industrial kitchens are feeling the pinch as energy costs soar and availability remains limited. The persisting situation could soon fuel domestic inflation and further strain household budgets.
access here

RBI Proposes Stronger Safeguards Against Digital Payment Fraud

The Reserve Bank of India (RBI) released a discussion paper proposing enhanced safeguards to curb the rising incidence of digital payment fraud. The proposals include a one-hour cooling-off period for high-value first-time digital transfers, a "kill switch" to instantly disable digital payment channels in case of fraud, and additional protections for senior citizens. These measures aim to strengthen India's digital financial ecosystem while ensuring greater consumer confidence and resilience against cyber-enabled financial crimes.
access here

Financial Intelligence Unit-India and Indian Cyber Crime Coordination Centre sign landmark MoU to combat cyber fraud and financial crimes

In a significant step towards strengthening India's economic and financial security, the Financial Intelligence Unit-India (FIU-IND) and the Indian Cyber Crime Coordination Centre (I4C) signed a Memorandum of Understanding to enhance intelligence sharing and operational coordination. The partnership aims to improve detection of financial crimes, support investigative agencies, facilitate asset recovery, and strengthen responses to cyber-enabled frauds, thereby reinforcing the country's anti-money laundering and cybercrime enforcement framework.
access here

The MoU was signed by Shri Amit Mohan Govil, Director, FIU-IND, and Shri Rajesh Kumar, Chief Executive Officer, the Indian Cyber Crime Coordination Centre (I4C)

RBI Expands Digital Rupee for Welfare and Cross-Border Payments

The Reserve Bank of India announced plans to expand the use of the digital rupee (CBDC) by extending pilot projects for government welfare schemes and cross-border payments. The initiative seeks to improve transparency, efficiency, and traceability in public expenditure while supporting secure international payment systems.
access here

RBI Warns of Global Risks but Highlights India's Resilience

In its May Bulletin, the Reserve Bank of India highlighted growing global risks arising from geopolitical tensions, elevated oil prices, rising public debt, and financial market volatility. Despite these external challenges, the RBI emphasised India's strong macroeconomic fundamentals, supported by healthy foreign exchange reserves, a resilient banking sector, stable inflation, and sustained domestic demand.
access here

SEBI Rejects Settlement Plea in Reliance Infrastructure Fund Diversion Case

The Securities and Exchange Board of India (SEBI) rejected settlement applications filed by Anil Ambani and Reliance Infrastructure in an investigation into the alleged diversion of company funds through related entities. SEBI's investigation concerns transactions amounting to thousands of crores that were allegedly routed to connected parties without adequate disclosures.
access here

AI-powered financial inclusion reshaping India's digital economy

India's financial inclusion journey is entering a new phase, powered by the convergence of Digital Public Infrastructure (DPI) and Artificial Intelligence, transforming how banking, lending, and financial services are delivered across the country. What began as a mission to provide basic banking access has evolved into a technology-driven ecosystem focused on real-time, intelligent, and inclusive financial services at scale. By leveraging digital footprints, consent-based data sharing, and advanced analytics, AI is enabling faster credit access, better risk assessment, enhanced security, and personalized financial services for millions of Indians.
access here

Supreme Court Closes Sterling Biotech Bank Fraud Case After Recovery

The Supreme Court approved a comprehensive settlement in the long-running Sterling Biotech bank fraud case after the promoters repaid nearly ₹9,800 crore to lending banks and deposited the remaining amount with the Court. Consequently, related criminal and regulatory proceedings were quashed.

The resolution marks one of India's largest recoveries in a banking fraud matter and highlights the evolving balance between financial recovery and criminal enforcement.
access here

Haryana Government Fund Diversion Case Sees Major Enforcement Action

Investigations into the alleged diversion of over ₹550 crore of Haryana Government funds intensified in April 2026, with two IAS officers suspended and the probe transferred to the CBI. The case involved suspected misuse of banking channels, forged financial instruments, and collusion among public officials and banking personnel. The matter underscores vulnerabilities in public financial management and the importance of robust internal financial controls.
access here

Authorities suspect that unauthorised payments were made using two accounts that had been opened with IDFC First Bank and AU Small Finance Bank.

ED Investigates Rajesh Exports for FEMA Violations

The Enforcement Directorate conducted searches at premises linked to Rajesh Exports in Bengaluru and Mumbai over alleged violations of the Foreign Exchange Management Act (FEMA). Investigators reported suspected irregular overseas trade transactions, opaque trade set-offs amounting to nearly ₹3,000 crore, inventory discrepancies, and possible offshore share manipulation.
access here

SEBI Tightens Oversight of Unregistered Investment Advisers

SEBI issued an enforcement order against Wealthmax Solutions Investment Advisor for alleged violations of investment adviser regulations. The order forms part of the regulator's continuing efforts to eliminate unauthorised financial advisory services, improve investor protection, and ensure that only registered professionals provide investment advice.
access here

ED Probes ₹356 Crore Bank Fraud Linked to Dhanlaxmi Solvex

The Directorate of Enforcement (ED), Indore Sub Zonal Office, has provisionally attached 19 immovable properties valued at ₹35.52 crore under the Prevention of Money Laundering Act (PMLA), 2002, in connection with a money laundering investigation involving M/s Dhanlaxmi Solvex Pvt. Ltd., its directors and associated entities. The investigation originated from a CBI FIR following a complaint by a consortium of banks alleging fraudulent availing of credit facilities and a wrongful loss of ₹356.31 crore. ED found evidence of alleged diversion and siphoning of loan funds through related entities, including circular trading, bogus transactions, accommodation entries and misuse of Letters of Credit.
access here

GST collections hit all-time high of over ₹2.42 lakh crore in April 2026

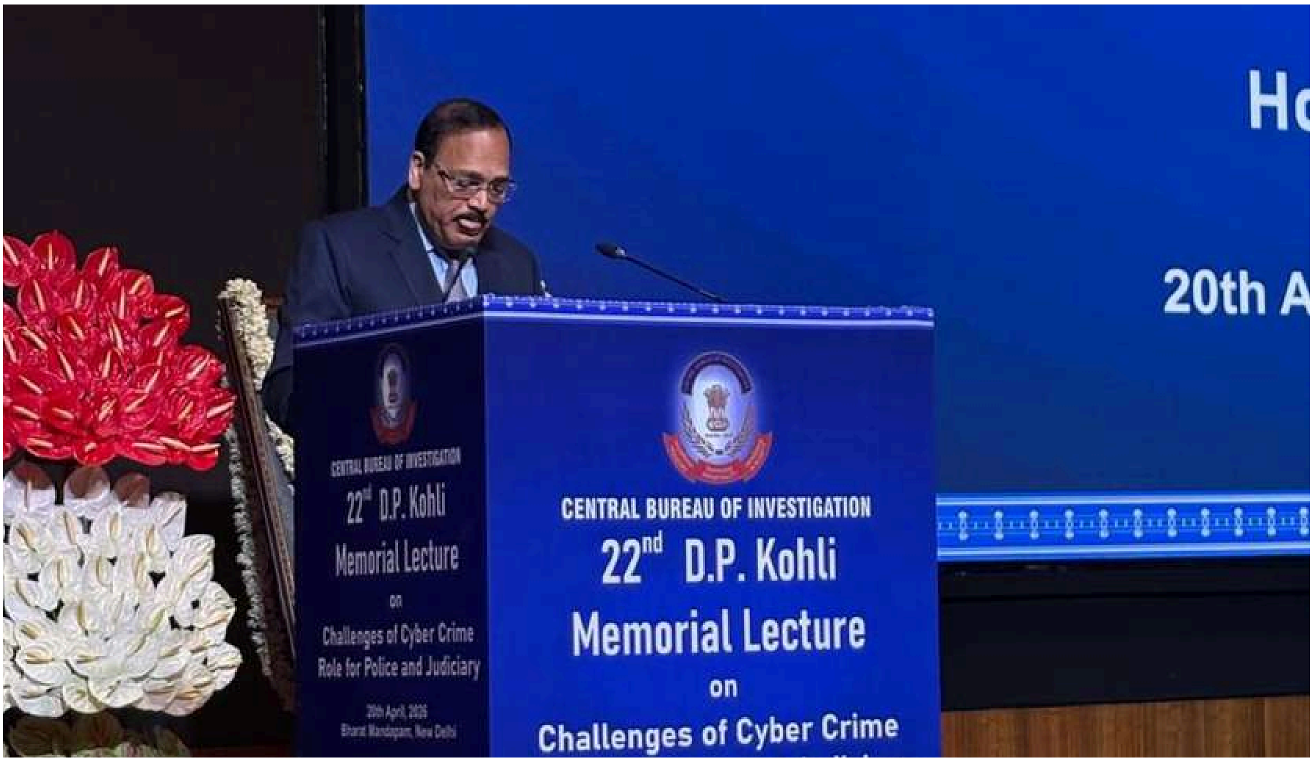
The Goods and Services Tax (GST) gross collections in April last month registered a record all-time high, growing 8.7 per cent as compared to the same period last year. The gross GST collection was recorded at over two lakh 42 thousand crore rupees, which was over two lakh 23 thousand crore rupees last year during the same month. The Gross Central GST collection in April last month stood at over 52 thousand crore rupees, and State GST was more than sixty-one thousand three hundred crore rupees. The gross Integrated GST (IGST) collection amounts to one lakh 29 thousand two hundred and 32 crore rupees.
access here

SFIO summons 4 Big Audit Firms over Rs 2,000 Crores IndusInd Bank's Derivatives Irregularities

According to the sources, the Serious Fraud Investigation Office (SFIO) has further increased the scope of the investigation in a big case related to IndusInd Bank. The case pertains to irregularities in the bank's derivatives portfolio, which is estimated to result in a loss of around Rs 2,000 crore. The investigation began when the bank itself reported in March 2025 that irregularities had been found in its derivatives transactions during the last 5 to 7 years.
access here

Participants of founding batch of Masters in Financial and Economic Crimes programme visit EAC-PM; Quarterly Newsletter on Economic Security Launched

Participants of the founding batch of the Master's in Financial and Economic Crimes (MFEC) programme visited the Economic Advisory Council to the Prime Minister (EAC-PM) recently as part of their Campus Immersion Programme, engaging in discussions on economic security, financial crime mitigation, and emerging threats to India's financial ecosystem. The interaction was attended by Prof. S. Mahendra Dev, Chairman, EAC-PM; Dr. K.K. Tripathi, Joint Secretary, EAC-PM; and Dr. Sri Vatsa Sehra, Joint Director, EAC-PM. The participants were accompanied by Prof. (Dr.) Naveen Sirohi, Programme Director of MFEC and Head of the School of Finance & Management at the Indian Institute of Corporate Affairs (IICA).
access here



Digital arrest is a crime against human dignity: CJI

Chief Justice Kant delivered the 22nd D.P. Kohli Memorial Lecture, organised by the Central Bureau of Investigation (CBI), on 'Challenges of Cyber Crime: Role of Police and Judiciary'.

The CJI flagged digital arrest scams as the "most disturbing" and lethal among cyber crimes, which not only result in merely financial loss to victims but also a "blistering sense of violation". He suggested measures such as real-time information-sharing frameworks, "briefly pausing" fund transactions to foreign accounts to verify the account holders, and integrated command structures capable of coordinating responses across sectors and agencies.
access here

Global News and Trends

India Assumes Historic Leadership Role at FATF, Strengthening Global Economic Security

A significant milestone in global financial governance was achieved as Giles Thomson (United Kingdom) assumed the Presidency of the Financial Action Task Force (FATF) for the 2026–2028 term, with Vivek Aggarwal, Secretary, Government of India, elected as FATF Vice-President for July 2026–June 2027.

This marks the first time India has held a leadership position in the global AML/CFT watchdog. India's appointment reflects international recognition of its robust anti-money laundering framework, successful FATF Mutual Evaluation, and growing contributions to global policy on digital payments, virtual assets, and illicit financial flows. The development strengthens India's role in shaping international standards for combating money laundering, terrorist financing, and emerging financial crime while advancing global economic and financial security.
access here

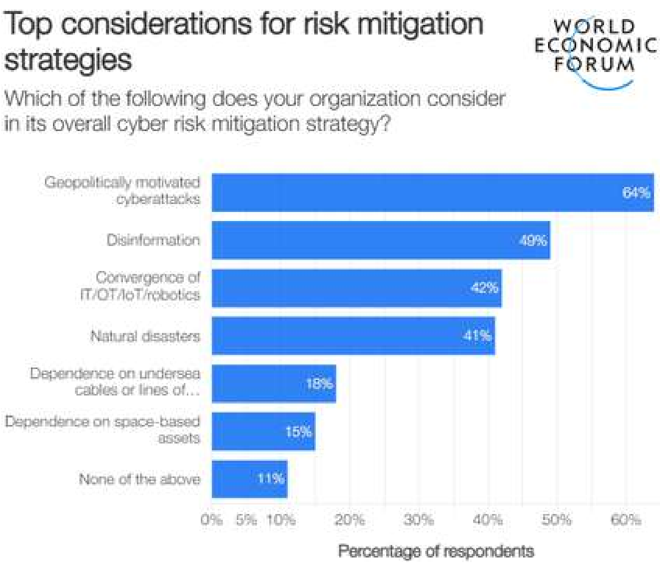
The Vice-President of the FATF

FATF Ministers Reaffirm Global Fight Against Illicit Finance

At the FATF Ministerial Meeting held alongside the IMF–World Bank Spring Meetings in Washington, member countries reaffirmed their commitment to combating money laundering, terrorist financing, proliferation financing, and the growing global threat of fraud. Ministers agreed to strengthen risk-based implementation of FATF standards, improve international cooperation, and enhance information sharing between governments and the private sector to safeguard the integrity of the international financial system.
access here

Cyberattacks target US infrastructure, and other cybersecurity news

A new joint advisory from US agencies has said that cyber activity targeting critical infrastructure has escalated in recent weeks amid the conflict in the Middle East, highlighting how geopolitical tensions are increasingly playing out in cyberspace. Hackers are exploiting internet-exposed operational technology (OT) devices — which are connected to the internet for remote monitoring, exposing infrastructure to attacks — used across sectors including energy, water and local government systems.
access here



IMF Flags AI-Driven Cyber Risks to Global Financial Stability

The IMF warned that artificial intelligence is increasingly being exploited by cybercriminals to identify software vulnerabilities and launch sophisticated cyberattacks against financial institutions. The Fund urged banks, regulators, and governments to strengthen cyber resilience, improve digital risk governance, and enhance international cooperation to mitigate emerging AI-enabled threats to global financial stability.
[access here](#)

Banks race to patch new cyber vulnerabilities, and other cybersecurity news

Banks in the US, EU and Japan are scrambling to fix cyber holes surfaced by Anthropic's Mythos AI tool, and to prepare for bad actors misusing tools of this type. While the vulnerability-hunting AI model has only been made available to a limited number of institutions currently, firstly in the US, its impact is being felt worldwide. Banks are discovering previously unknown weaknesses, increasing pressure to accelerate remediation and upgrades, particularly in institutions with ageing legacy systems. Smaller banks are being warned through shared findings from larger peers, while the European Central Bank (ECB) is urging banks across the eurozone to urgently prepare for cyberattacks. "Lack of access [to Mythos] is no excuse for doing nothing. On the contrary, it makes it even more important for banks to act now," said ECB Executive Board member Frank Elderson.
[access here](#)

Global Regulators Increase Focus on AI-Driven Financial Crime

Cyber incidents are escalating in magnitude, sophistication and geopolitical relevance, exposing critical weaknesses in the global financial system. This paper highlights three mutually reinforcing vulnerabilities: supply chain/third-party exposure, heightened systemic risk in rapidly digitalising developing regions, and strong timing effects that amplify shocks during market stress. The paper also recognises that cybersecurity extends beyond a purely technical concern and has broader macro-financial and economic-security implications. Finally, the paper emphasises a set of measures for financial firms and financial sector supervisors to contain propagation channels, safeguard confidence and reinforce financial stability.
[access here](#)

Expert Discussion "Economic Security of Ukraine in the New Global Architecture of Risks"

The discussion focused on key issues of economic security, including: transforming economic security into a tool of practical public management in the context of a protracted war and global fragmentation, assessing the real state of economic security, reducing critical dependencies on external financing, strengthening the state's institutional capacity in the field of economic security, mobilizing internal resources, preserving human capital, and directing reconstruction toward the industrial and technological development of Ukraine.

access here

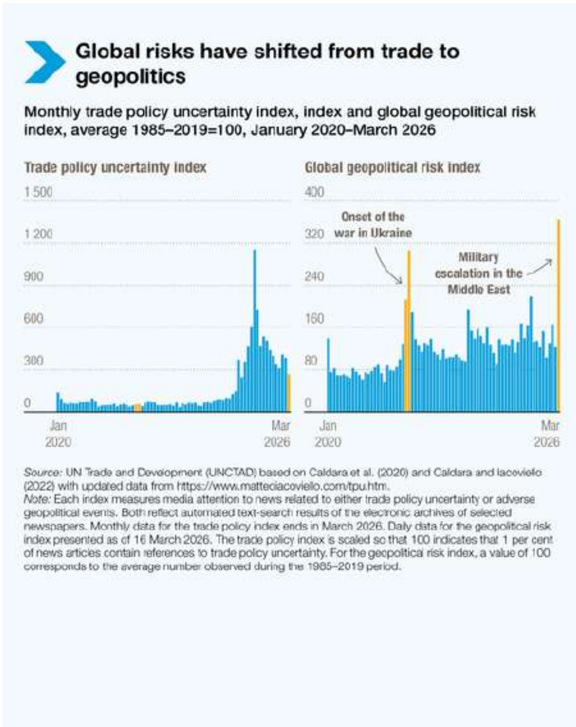
The National Institute for Strategic Studies held a hybrid expert discussion on 10 June 2026, "Economic Security of Ukraine in the New Global Architecture of Risks", accompanied by the presentation of an analytical report of the Institute's Centre for Economic and Social Studies.

Global economy faces new test as trade, food and finance shocks spread

The global economy entered 2026 with resilience, supported by trade, industrial production in developing economies and investment linked to artificial intelligence (AI). But rising geopolitical tensions are now testing that momentum, according to UN Trade and Development (UNCTAD).

UNCTAD's 'Trade and Development Foresights 2026: Global economy faces a geopolitical challenge' warns that the global economy is moving from an initial phase of supply disruptions and inflation into a more fragile period, where prolonged uncertainty could trigger shortages and wider financial stress. While recent years were shaped largely by trade tensions and policy uncertainty, geopolitical risks are now becoming the dominant source of instability for the global economy.

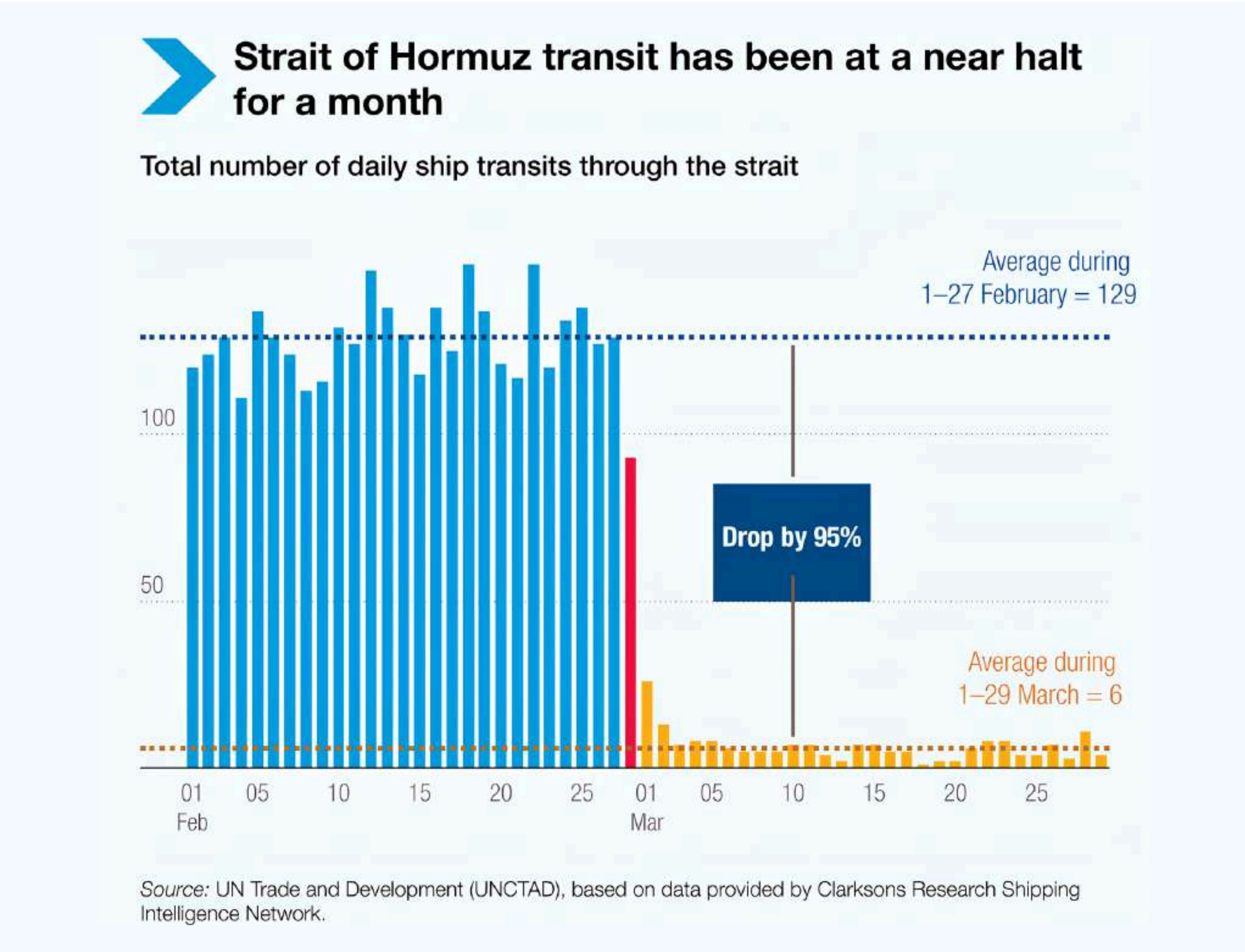
access here



Hormuz disruption deepens global economic strain across trade, prices and finance

The Strait of Hormuz remains virtually closed, with effects spreading through the global economy within weeks by disrupting energy flows, raising prices and increasing financial pressure on developing countries, UN Trade and Development (UNCTAD) warns in its second rapid assessment. What began as a disruption in a key energy corridor is now feeding through the entire global economy.

The update follows an initial assessment issued on 10 March and confirms a rapid worsening of global conditions since the escalation at the end of February, with risks now extending well beyond energy markets
access here



Financial Action Task Force's June 2026 Working Group and Plenary

Treasury officials participated in the June Plenary meeting of the Financial Action Task Force (FATF), the global standard-setting body for anti-money laundering, countering the financing of terrorism, and proliferation of weapons of mass destruction.

FATF members agreed to take further steps to combat fraud and encourage risk-based supervision of the international financial system. The group adopted mutual evaluations of Canada and Türkiye, as well as reports urging better information sharing with the private sector. To assist the private sector in assessing risk and sharing information, the FATF agreed to publish several typology reports on emerging risks, such as the abuse of online gaming and vulnerabilities related to underground banking.
access here

Fraud: An Economic and National Security Threat

The Crime Survey for England and Wales (year ending December 2025) estimated 4.4 million fraud incidents. Out of the estimated 4.4 million incidents of fraud, around 3.2 million incidents involved a loss. Victims said that they were fully reimbursed in 2.4 million of these cases. Levels of fraud have increased by 30% since the earliest comparable year, the year ending March 2017.

Fraud is a rapidly growing global issue, becoming more sophisticated, cyber-enabled and frequently crossing borders. Threats include authorised push payment, account takeover, romance scams, application fraud, chargeback fraud, payment card fraud, money mules and investment scams. Although these frauds look different at the point of loss, many rely on the same underlying infrastructure. For example, compromised credentials, mule accounts, synthetic identities, manipulated communications, weak onboarding controls, fragmented customer data and cross-border criminal networks.
access here

Financial losses from scams hit £1.3bn a year as criminals turn to AI

Cases of fraud in the UK have surged with criminals using AI to manipulate people and even marrying victims of romance scams to steal more money. More than four million cases in which money was lost were reported last year - the equivalent of nearly eight on average every minute, according to new figures. The total has increased by more than one million in two years, with almost £1.3bn stolen by scammers in 2025, according to an annual report by UK Finance.

The enormous scale of the problem could only be tackled if tech companies stepped up monitoring and security of their platforms, the banking trade body said.
access here

International Conference on Economic Crime

The Serious Fraud Office hosted an International Economic Crime Conference in collaboration with France's Parquet National Financier (PNF) and Switzerland's Office of the Attorney General (OAG). The event was held over two days at Drapers' Hall in central London, bringing together over 100 investigators and prosecutors from multiple jurisdictions.
access here

Events at IICA

Economic Security Insights: Quarterly Newsletter Launched by EAC-PM

The Indian Institute of Corporate Affairs (IICA) launched "*Economic Security Insights*", a quarterly newsletter aimed at fostering informed dialogue and advancing thought leadership on issues of financial and economic security.

The inaugural issue was formally launched on 18th June 2026 at NITI Aayog, New Delhi, by Prof. S. Mahendra Dev, Chairman, EAC-PM, in the presence of Dr K.K. Tripathi, Joint Secretary, EAC-PM, and Dr Sri Vatsa Sehra, Joint Director, EAC-PM. The IICA delegation was led by Prof. (Dr) Naveen Sirohi, Head, School of Finance & Management, IICA.

Conceptualised as a dedicated knowledge platform, the newsletter seeks to contribute to contemporary discourse at the intersection of finance, governance, regulation, public policy and national economic security. As economies become increasingly interconnected and financial risks continue to evolve in complexity and scale, the publication aims to encourage deeper engagement with emerging challenges and the strategic responses that shape economic resilience.

Through expert perspectives, policy analysis, and thematic insights, Economic Security Insights will focus on strengthening understanding of financial integrity, regulatory developments, institutional preparedness, and intelligence-led approaches to addressing financial and economic threats.

The initiative reflects IICA's continued commitment to strengthening knowledge ecosystems through research, capacity building and policy engagement in support of India's evolving economic security priorities. The visit to EAC-PM was part of the campus immersion program for the participants of the Master's in Financial and Economic Crimes (MFEC) .

https://iica.nic.in/mfes

Masters in Financial and Economic Security (MFES)

With the rapid expansion of digital economies and cross-border financial transactions, financial and economic crimes such as money laundering, cyber fraud, corporate misconduct, procurement fraud, and other complex financial offences have grown significantly in scale and sophistication. These evolving threats pose serious challenges to national security, institutional integrity, market confidence, and economic stability. Addressing these challenges requires a new generation of professionals equipped with interdisciplinary expertise in financial forensics, investigative methodologies, regulatory and legal frameworks, risk management, and emerging technologies. Recognising this critical national imperative, Rashtriya Raksha University (RRU), in collaboration with the Indian Institute of Corporate Affairs (IICA), has designed the Master's in Financial and Economic Security, a flagship programme aimed at **developing a specialised cadre of professionals capable of preventing, detecting, investigating, and mitigating financial and economic crimes, thereby strengthening India's economic security architecture.**

PROGRAM FEATURES

12 Months Hybrid Program
Comprehensive training spread over twelve months

10 Modules
Extensive curriculum covering theoretical and practical aspects

Live Online Classes
Interactive learning through live online sessions with recordings

Alumni Connect
Join a growing network of global professionals

250+ Hours Delivery
In-depth learning through interactive sessions

2 Campus Immersions
In-person campus immersions at IICA and RRU campuses

Site Visits
Practical exposure through relevant site and institutional visits

Practitioner Centric
Case studies, simulations, and real-world insights

Global Experts
Learn from global faculties and renowned practitioners

Support and Resources
e-libraries, professional tools, and global collaboration opportunities

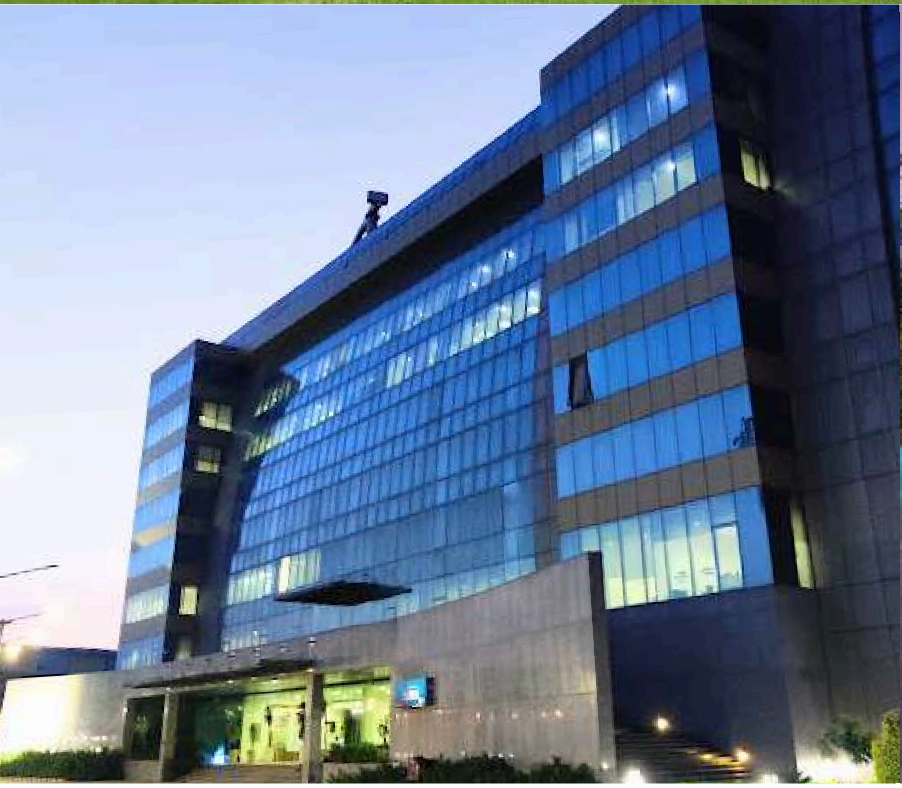
FEE STRUCTURE

Registration Fee (Non-Refundable)	**Indian Nationals:** ₹5,000/- **Foreign Nationals:** USD 100
Program Fee (Lump-Sum)	**Indian Nationals:** ₹3,60,000/- **Foreign Nationals:** USD 5,000

For registration, kindly contact:

Prof (Dr) Naveen Sirohi
Program Director (IICA), MFES
Email: mfes@iica.in / sof@iica.in
Mobile/WhatsApp: +91 98188 55826

Ms. Anjali Yadav
Chief Program Executive (IICA), MFES
Email: cpe.sofm@iica.in
Mobile/WhatsApp: +91 98118 68172



TEAM

Prof (Dr) Naveen Sirohi
HoD, School of Finance
Email: naveen.sirohi@iica.in

Anjali Yadav
Chief Program Executive
Email: cpe.sofm@iica.in

Abbas
Chief Program Executive
IICA

Abhishek Kaushal
Senior Consultant
IICA

Kaushal Kumar
Consultant
IICA

School of Finance and Management
Indian Institute of Corporate Affairs
Plot P 6,7 and 8, Sector 5, IMT Manesar, Gurugram, Haryana-122052
Phone: 0124-2640080 | Email: sof@iica.in | www.iica.nic.in