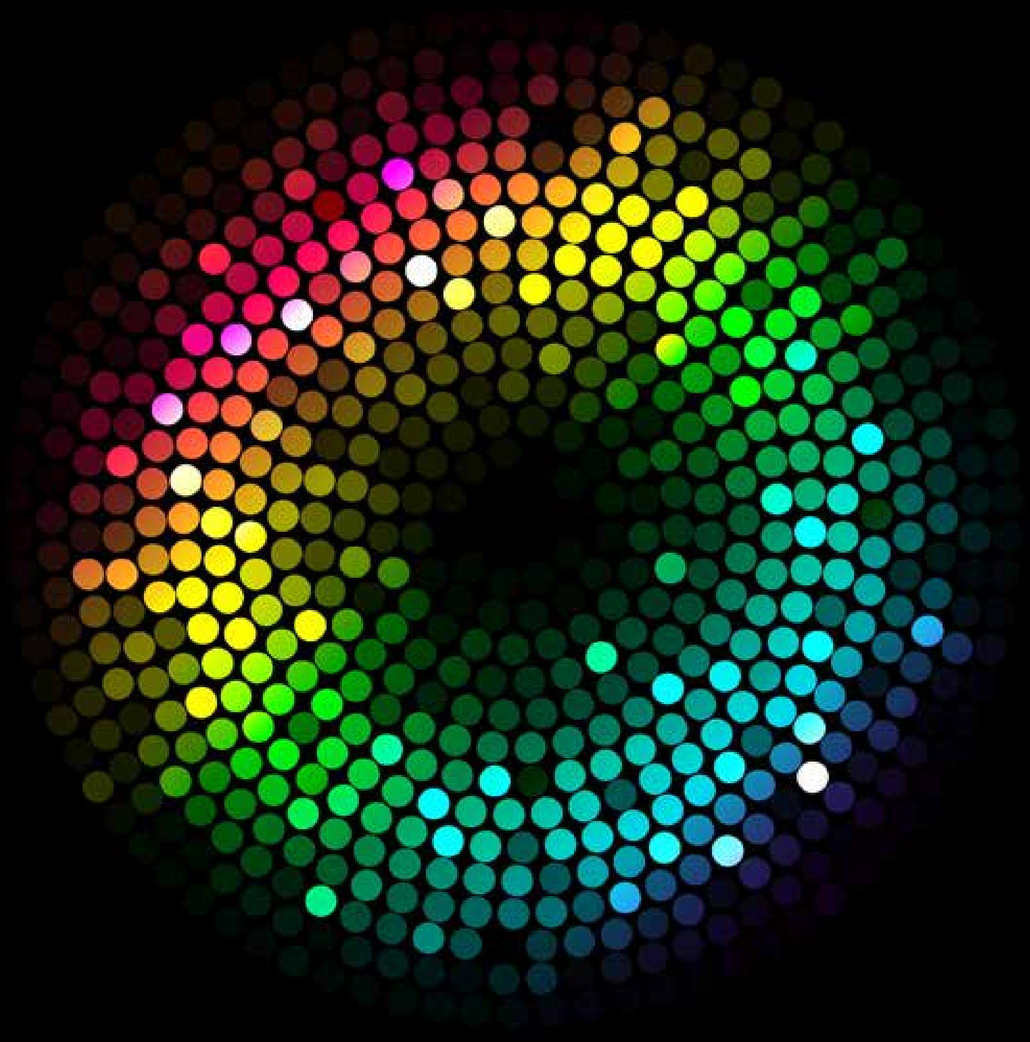
Deloitte.



Compliance under the Economic Crime and Corporate Transparency Act, 2023

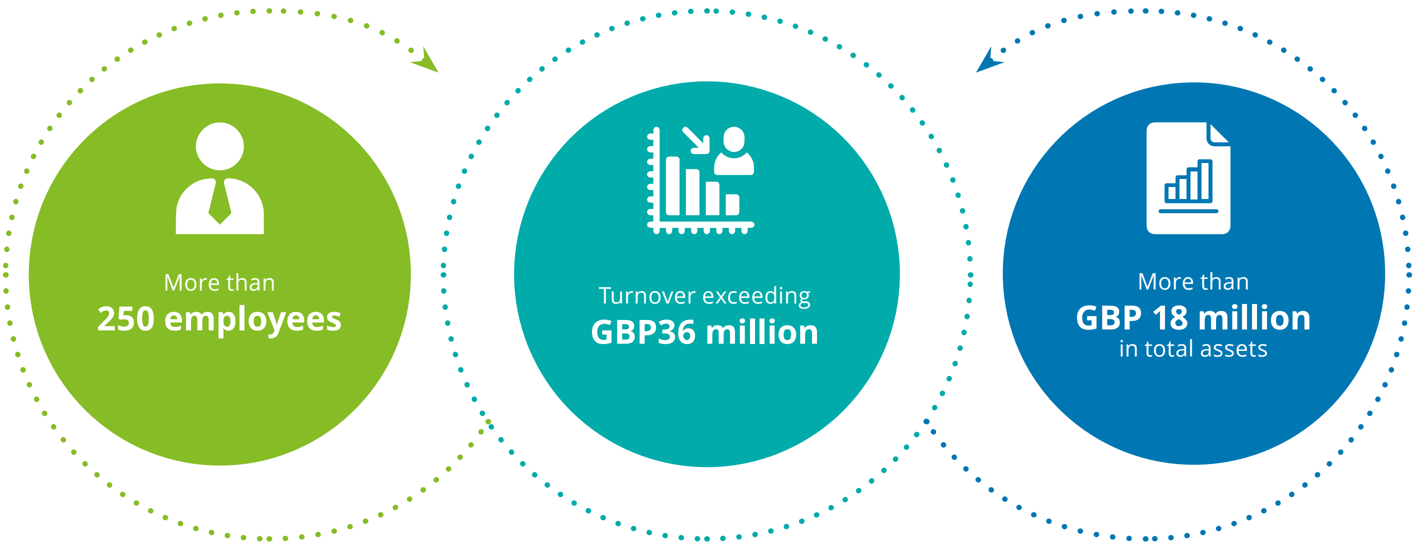
A guide for Indian businesses

June 2025

The Economic Crime and Corporate Transparency Act 2023 (ECCTA) marks a transformative development in the UK's legal landscape, introducing stricter corporate conduct obligations, particularly fraud prevention. The Act aims to improve corporate transparency and tackle financial crimes, including fraud and wider economic crimes, by holding companies accountable for failing to prevent such offences. The ECCTA introduces a new corporate offence, Failure to Prevent Fraud (FTPF), which will take effect from 1 September 2025. For Indian businesses with nexus in the UK, this presents both a compliance challenge and an opportunity to reinforce ethical standards and enhance global credibility.

A new era of corporate accountability

Currently, FTPF applies to large organisations that meet at least two of the following criteria:



Although currently limited to large businesses, the UK government has indicated it may revise these thresholds, potentially bringing smaller organisations within this scope.

UK nexus: Global reach and extraterritorial implications

While the Act is a UK law, its extraterritorial reach means that Indian companies with a UK presence, or those operating as subsidiaries or service providers to UK entities, may also be affected. Similarly, UK companies operating in India must assess their exposure to fraud risks from associated persons within the Indian jurisdiction. In essence, even if the fraud is perpetrated outside the UK, any resulting gain or loss within the UK is enough to establish a UK nexus.

Understanding the FTPF offence

The FTPF offence marks a significant shift in fraud compliance. Historically, fraud prevention efforts have focused on safeguarding organisations from being victims. Now, the emphasis is on frauds committed for the benefit of the organisation, even if the benefit is never actually realised.

An organisation will be criminally liable if:

- Fraud is committed by an "associated person" (employees, agents, international distributors or third-party representatives acting on behalf of the organisation).
- The fraud was intended to benefit the organisation or its clients.
- The organisation did not have reasonable fraud prevention procedures in place.

This liability applies even if:

01 Senior management had no knowledge of the fraud.

02 Senior management was not involved in the fraud.

The offence also applies when:

- The benefit is intended but not realised.
- The organisation is both a beneficiary and a victim, such as gaining short-term profits from fraud but suffering reputational damage later.

The law also broadens the traditional "identification principle" by holding companies liable for actions taken by any senior manager, defined as anyone who plays a significant role in managing or organising a substantial part of the company's activities.

Key implications for Indian businesses

Indian subsidiaries of large UK companies and organisations (which meet the predefined criteria) with operations, clients or collaborations in the UK or serving UK-based companies, should consider the following:

01 Assess their exposure to fraud risks from associated persons (including third parties) in India.

02 Strengthen their anti-fraud frameworks, including policies, controls and response mechanisms (such as whistleblowing channels).

03 Evaluate and enhance their due diligence practices for third parties.

04 Invest in technology solutions such as fraud detection tools and data analytics to monitor transactions and identify patterns indicative of potential fraud.

05 Conduct training sessions for employees on the application and implications of the ECCTA.

06 Ensure that their fraud prevention methods are commensurate with their business's size, scale and maturity.

Reasonable procedures and compliance principles

The guidance outlines six principles to help organisations develop “reasonable procedures” to prevent fraud. While non-prescriptive, these principles are essential for any business seeking to build a defensible anti-fraud framework:

Top-level commitment: Ensure leadership sets the tone from the top and supports a culture of integrity and compliance.

Due diligence: Apply risk-based due diligence on associated persons to identify and mitigate potential fraud threats.

Risk assessment: Periodically assess fraud risks, focusing on activities and relationships most susceptible to misuse.

Communication (including training): Promote fraud awareness and provide tailored training to employees and associated persons.

Proportionate risk-based prevention procedures: Design policies and controls that are proportionate to the business's size, scale and maturity.

Monitoring and review: Regularly test and improve prevention measures in response to changing risks and incidents.

Interpreting liability under the ECCTA

Fraud with a UK nexus by a foreign entity

Scenario
A UK Government grant programme subsidises heating appliances that meet certain efficiency standards. A small UK-based manufacturer sends its appliances to an overseas testing laboratory for efficiency verification. The laboratory, although not located in the UK, is aware that only appliances surpassing a specified threshold will qualify for grants. To ensure eligibility, the lab manager falsifies test data to reflect higher efficiency ratings.

Analysis
This constitutes fraud by false representation by the overseas laboratory manager, who is an associated person acting on behalf of the laboratory. As a result of the falsified results, the UK manufacturer gains an unfair financial advantage.

Implication under ECCTA
Despite being located outside the UK, the international testing company may be prosecuted under Section 199(1)(b) due to the fraud with a UK nexus—i.e., the fraudulent act benefits a UK entity. The company would need to demonstrate that it had reasonable procedures to prevent such fraud to avoid liability.

Fraud by abuse of position

Scenario
In Company A, the payroll department ensures monthly contributions are made to employees' pension funds. However, the head of the payroll department diverts a portion of these payments to fund other internal projects, while continuing to record them as legitimate pension contributions.

Analysis
This constitutes fraud by abuse of position, as the individual, entrusted with fiduciary responsibilities, deliberately misuses their position for an improper purpose. The associated person in this case is the head of payroll.

Implication under ECCTA
Although the diverted funds were used for internal purposes, Company A could be held liable under Section 199(1)(a) of the ECCTA, unless it can demonstrate that it had reasonable fraud prevention procedures in place at the time of the misconduct.

Aiding and abetting fraud

Scenario
Company A seeks financing from a bank to purchase new equipment. To strengthen their case for the borrowing, Employee C of Company A persuades a client, Company B, to issue a letter to the bank falsely stating that it intends to place future orders with Company A once the equipment is acquired. Employee C even drafts the letter for Company B's signature. In truth, Company B is winding down its operations and has no intention of placing any orders, making the representation knowingly false and intended to mislead the bank.

Analysis
Company B commits fraud by false representation, knowingly issuing a misleading statement to influence the bank's lending decision. By orchestrating and facilitating the misrepresentation, Employee C is guilty of aiding and abetting the fraud. The fraud was carried out with the intent to benefit Company A.

Implication under ECCTA
Even though Company A did not directly commit the fraud, it could still be held liable under the ECCTA, given that the fraudulent act was intended to benefit the organisation. Liability would apply unless Company A can prove it had adequate procedures in place to prevent such conduct by its associated persons.

Source: https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version#chapter-2overview-of-the-offence'

Summary of liability under the ECCTA

Who commits the base fraud	Who is intended to benefit	Who could be prosecuted for failure to prevent the base fraud
An associated person	The relevant organisation	The relevant organisation
An associated person	The clients of the relevant organisation to *whom* the associated person provides services for or on behalf of the relevant organisation	The relevant organisation, except where it is the victim or intended victim of the base fraud [Section 199(3)]
An associated person	The clients of the relevant organisation, *where* the associated person provides services to subsidiaries of those clients for or on behalf of the relevant organisation	The relevant organisation, except where it is the victim or intended victim of the base fraud [Section 199(3)]
The employee of a subsidiary of a large parent organisation	The subsidiary	The subsidiary
The employee of a subsidiary of a large parent organisation	The parent organisation	The parent organisation

Source: https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version#chapter-2overview-of-the-offence

Steps for effective implementation

To successfully align with the requirements of the ECCTA, Indian businesses should take a proactive, structured approach to compliance. Key steps include:

01 Building a culture of compliance and ethics

Evaluate the effectiveness of current fraud prevention measures:
Organisations should consider initiating exercises to evaluate their anti-fraud policies and frameworks. ECCTA expects large organisations to have reasonable and proportionate measures to prevent fraud.

Implement tailored training programmes:
Provide regular, role-specific training to employees on fraud risks, ethical business practices and compliance obligations, along with potential liabilities under ECCTA. Tailor content to reflect the unique risk exposures of different departments. Targeted education can help foster a deeper understanding of fraud risks and ethical expectations, ensuring employees across the organisation are equipped to act responsibly.

Establish confidential whistleblower mechanisms:
Establish confidential, retaliation-free channels for employees and/or third parties to report suspected fraud or misconduct. Such mechanisms can help foster a culture of transparency and accountability, encouraging early detection and resolution of unethical behaviour.

02 Strengthening controls and risk management

Conduct a comprehensive fraud risk assessment:
Evaluate existing policies and procedures against the standards set by ECCTA on a regular basis. A detailed review of the fraud control framework will be required at regular intervals to help identify compliance gaps and highlight areas that require immediate attention or improvement.

Develop robust anti-fraud policies:
Establish clear and enforceable anti-fraud policies that define expected employee conduct and outline procedures for detecting and responding to fraud. Ensure these policies are well-documented and communicated across the organisation.

Strengthen due diligence processes:
Implement rigorous vetting procedures and enhanced due diligence methods when onboarding/working with third-party vendors, agents, etc., especially those with nexus in the UK. Include specific clauses in contracts mandating adherence to anti-fraud and compliance standards.

Ongoing regulatory monitoring:
Obtain necessary legal advice and stay abreast of updates related to the ECCTA and other applicable UK/anti-bribery and anti-corruption regulations. Proactive and continuous monitoring can help ensure timely adjustments to compliance strategies, reducing the risk of inadvertent non-compliance.

03 Using technology to prevent and detect fraud

Invest in digital/technology solutions: Adopt advanced tools such as fraud detection systems and data analytics platforms to enable real-time monitoring and early identification of suspicious transactions or patterns.

Conclusion

The ECCTA sets a new standard for corporate accountability. Indian businesses subject to the ECCTA need to act now by embedding ethics into their culture, strengthening controls, training teams and investing in technology.

By acting proactively and implementing these measures, Indian companies can mitigate legal risks and enhance their reputation as ethical and trustworthy global players, thereby gaining a competitive advantage.

As the enforcement date of 1 September 2025 approaches, organisations should accelerate their readiness to meet the expectations of this landmark legislation. Indian companies must remain vigilant, adaptable and committed to upholding the highest standards of corporate conduct, ensuring long-term growth and resilience in an increasingly regulated international business environment.

Connect with us

Nikhil Bedi
Partner and Leader – Risk, Regulatory & Forensic
Strategy, Risk & Transactions
Deloitte India
nikhilbedi@deloitte.com

K.V. Karthik
Partner and Leader – Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
kvkarthik@deloitte.com

Saurabh Khosla
Partner - Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
khoslas@deloitte.com

Stacey Toder Feldman
Partner - Risk, Regulatory & Forensic
Strategy, Risk & Transactions
Deloitte UK
stoderfeldman@deloitte.co.uk

Contributor

Chirayu Ghai (Deloitte UK)