Deloitte.

Together makes progress

Fraud and Corporate Misconduct Watch

Harnessing AI and data to manage conflict of interest risk|October 2025

In a Southeast Asian subsidiary of a multi-national conglomerate, a procurement officer quietly awarded contracts to his brother-in-law's company. No alarms were raised. The vendor onboarding process appeared to have been followed-on paper. It took a whistleblower to expose the hidden relationship and trigger an internal investigation.

In today's hyper-connected business world, conflicts of interest (CoI) like these are rarely obvious-but they have potentially damaging repercussions.

This is a familiar scenario for many of the investigations that Deloitte conducts for clients across Southeast Asia. CoI, particularly in procurement, can severely undermine the integrity of processes leading to unfair advantages, preferential treatment, and even corruption. It is crucial therefore for an organisation to understand where it may be exposed to CoI, from the obvious to the subtle, so the risks can be mitigated.

Actual conflict – Direct conflict where an employee's / vendor's private interest has influenced their professional duties.

Apparent/perceived conflict – Reasonable ground to believe that an employee's / vendor's private interests may improperly influence their professional duties.

Potential conflict – Conflict could arise in the future. No bias may have occurred yet, but the potential is there.

CoI occur when personal interests or those of close connections intersect with professional duties. They are relationships and not actions on their own. Trust, both within and outside the organisation, is compromised when such relationships lead to biased decision-making and a loss of objectivity. In today's complex business environment, CoI are inevitable and while they may be common, how an organisation identifies, manages, and mitigates these conflicts can impact its credibility and long-term success.

Traditional mitigation strategies such as annual declarations and manual reviews are no longer sufficient. They rely on self-reporting and static controls, often missing hidden relationships or evolving risk patterns.

What are the red flags?
When it comes to an undisclosed conflict of interest, how can an organisation spot if an individual has failed to act in the best interest of the employer but rather acted for their own benefit? Some red flags to look out for include:

• Financial and business red flags
Unexplained financial gains:
A sudden display of significant and unexplained lifestyle changes such as purchase or possession of luxurious products, expensive gifts and frequent travel that does not align with the employee's income or a corresponding change in compensation.

Suspicious vendor relationships:
Contracts being consistently awarding to the same vendor without proper evaluation or clear justification.

Unusual decision-making patterns:
Deviation from or bypassing standard procedures (skipping approvals, one employee dominating decisions that should involve broader parties).

• Behavioural and relational red flags
Favouritism:
Employees hire or promote an unqualified individual.

Misuse of position:
Using confidential company information for personal gain (insider trading) or taking advantage of a business opportunity that the company could have pursued.

Why is mitigating conflicts of interest important?

Failure to address CoI may lead to severe repercussions for an organisation. Internally, this includes erosion of trust as well as low morale, resentment and damage to the organisation's culture. Externally, it could have reputational damage leading to loss of customers, investors and business partners.

In some cases, CoI may lead to legal issues and regulatory scrutiny being thrust upon the organisation. In Southeast Asia, there are various rules and regulations related to CoI, some of which include Indonesia's Law No. 31/1999 on Corruption Eradication[1], Bursa Malaysia Listing Requirements[2], Decree 59/2019 of Vietnam's 2018 Anti-Corruption Law[3], and Section 156 of Singapore's Companies Act (Cap. 50).[4] Going a step further, the UK's Failure to Prevent Fraud[5] offence has recently come into effect and is likely to raise the bar for compliance internationally, much like the UK Bribery Act 2010 did.

> As CoI can be a conduit for fraud, organisations should include conflict of interest management as part of their fraud prevention procedures to mitigate risk and demonstrate compliance.

This is emphasised by the recently released ISO 37009[6], a standard for managing CoI in organisations. The standard provides guidance to organisations on understanding CoI and how to manage the risk based on the principles of trust, integrity, transparency and accountability. It distinguishes and provides guidance on dealing with actual, apparent/perceived and potential CoI.

To stay ahead, organisations must implement a policy framework that consistently identifies, manages and mitigates all CoI risks to a reasonable level. ISO 37009 states that CoI can be identified from a variety of sources. These include CoI disclosures, risk analysis, audits and incidents within the organisation.

Effective management involves assessing disclosed information to understand the nature and potential impact of the conflict and then determining the appropriate course of action based on the assessed risk level. Organisations should also ensure enforcement of consequences for non-disclosure or violation of CoI policies. With mitigation, controls such as separation of duties are important safeguards. This should be complemented with regular training sessions to raise awareness. Above all, the organisation should foster an ethical and transparent environment which encourages reporting of undisclosed conflicts without fear of retaliation.

Taking the next step with a proactive data driven approach
While the policy framework sets the foundation for managing the risk associated with CoI, it can be limited in addressing the nuances of human behaviour. To address this, the framework should go beyond policies in harnessing the power of data to conduct insightful analytics. By combining internal and external data sources, organisations can build a holistic and proactive view of potential conflicts and take necessary remedial actions.

1   https://cms.kpk.go.id/storage/3932/uu311999.pdf
2   https://www.bursamalaysia.com/sites/5bb54be15f36ca0af339077a/content_entry5ce3b5005b711a1764454c1a/64702cad39fba2588757656a/files/Appendix_2_ICN_COI_Guidance.pdf
3   https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=197302
4   https://sso.agc.gov.sg/Act-Rev/CoA1967/Published/20211231?DocDate=20061031
5   https://www.gov.uk/government/news/new-measures-to-tackle-fraud-come-into-effect
6   https://www.iso.org/standard/74095.html

Proactive detection using analytics: The power of GenAI

Deloitte's generative artificial intelligence (GenAI) based approach to proactively detect CoI between employees and vendors/third parties moves beyond traditional rule-based methods in data analytics. It connects vast, complex, unstructured internal and external data. By leveraging GenAI and advanced analytics, organisations can transform how they manage the risk. These tools enable continuous monitoring and proactive risk identification—far beyond what traditional methods to proactively detect CoI can achieve.

Deloitte's Conflict of Interest Analytics

Advanced data aggregation & cross-referencing

- GenAI, using NLP capabilities, can ingest and analyse structured data (e.g., transaction records, vendor and employee master files etc.) and unstructured data (e.g., adverse media, public database records etc.).
- Detect hidden relationships by cross-referencing names, organisations, contact numbers, addresses etc. across large datasets to identify overlaps and connections that a human or simple query would likely miss.

Sophisticated pattern & anomaly detection

- GenAI models excel at spotting deviations from "normal" organisational or individual behaviour (e.g., vendors awarded business soon after establishment date, vendors with a high share of business, vendors with concentrated revenue risk etc.).
- Detect behaviour changes across procurement (e.g. supplier shifts, recent gain of business share etc.).

Continuous monitoring

- GenAI can continuously monitor conflicts of interest by integrating with Enterprise Resource Planning (ERP) databases to prompt human review and immediate action.
- The weighted potential conflict risks determined allow for prioritisation of alerts and offer a 360 degree view of the risk to the investigator.

Strategic benefits

By deploying Deloitte's Conflict of Interest analytics, clients gain the following benefits:

Fraud prevention
- Helps uncover hidden relationships that may indicate fraudulent behaviour such as collusion, kickbacks, or bid rigging.

Transparency in vendor relationships
- Prevents biased vendor selection, ensuring a fair and competitive procurement process.
- Demonstrates good corporate governance.
- A well-defined analytics program strengthens the organisation's compliance program and provides tangible proof to regulators, investors, and the public that the organization is serious about risk management and ethics; especially when facing regulatory scrutiny.

Improved decision making
- Promotes merit-based practices and reduces favoritism, leading to better outcomes in hiring, procurement, strategy and investments.

Minimise financial losses
- Enables timely detection of suspicious activities to minimise financial leakage.
- Controls spending risks by identifying vendors or transactions with high CoI risk.
- Reduces the risk of regulatory penalties, litigation, contract breaches and loss of revenue from reputational damage due to undisclosed conflicts surfacing in the public domain.

Next steps
CoI are no longer just ethical dilemmas—they are operational, reputational, and regulatory risks. Organisations must move beyond passive compliance and embrace proactive, data-driven strategies to detect and manage CoI. By leveraging GenAI-powered analytics, leaders can uncover hidden relationships, strengthen governance, and protect stakeholder trust. The time to act is now: review your current policy framework, assess your data capabilities, and ask—are you truly seeing the full picture when it comes to CoI?

Contacts

Jarrod Baker
Forensic & Financial Crime Partner
Deloitte Southeast Asia
jarbaker@deloitte.com

Doddy Ashraf Zulma
Forensic & Financial Crime Partner
Deloitte Indonesia
dzulma@deloitte.com

OoYang Ping
Forensic & Financial Crime Partner
Deloitte Malaysia
yoo@deloitte.com

Eiichi Yoshikawa
Forensic & Financial Crime Director
Deloitte Thailand
eyoshikawa@deloitte.com

Hanh Do Thi Hong
Forensic & Financial Crime Director
Deloitte Vietnam
hanhdo@deloitte.com

Kunall Kohli
Forensic & Financial Crime Senior Manager
Deloitte Singapore
kunakohli@deloitte.com

About Deloitte Forensic & Financial Crime

Treating potential business threats today to help protect you against risk tomorrow
With increasing regulation and technology-fueled financial crime, threats to the reputation and value of your business are widespread.

That's why we are ready to help you address issues related to financial crime, fraud, and corporate misconduct. Our world-class team of specialists leverage the depth and breadth of Deloitte's global presence alongside innovative technology and tools, like GenAI, to deliver tailored solutions that support discovery services through litigation and regulatory matters, investigation management around data and disputes, fact-finding services, business disputes, and claims management.

From resolving business crises, controversies, and transactions to treating potential business threats today, we protect brands, reputations, and communities around us by proactively advising on exposure to fraud, corruption, money laundering and other financial crime issues. By working with us, be empowered to drive progress and champion the unexpected.

Our Southeast Asia team
With Deloitte operating as an integrated firm in Southeast Asia, our team of over 200 forensic professionals provides fraud and investigation, discovery and computer forensic, data analytics and financial crime advisory services seamlessly across the region. Our local team has extensive experience in performing prominent and challenging engagements across industries and in   many countries. In countries where we do not have dedicated forensic professionals, we team with the local Deloitte office to provide local language and cultural expertise.

Deloitte.