Economic Crime and Corporate Transparency Act 2023
Fraud Risk Assessment Tool

Introduction

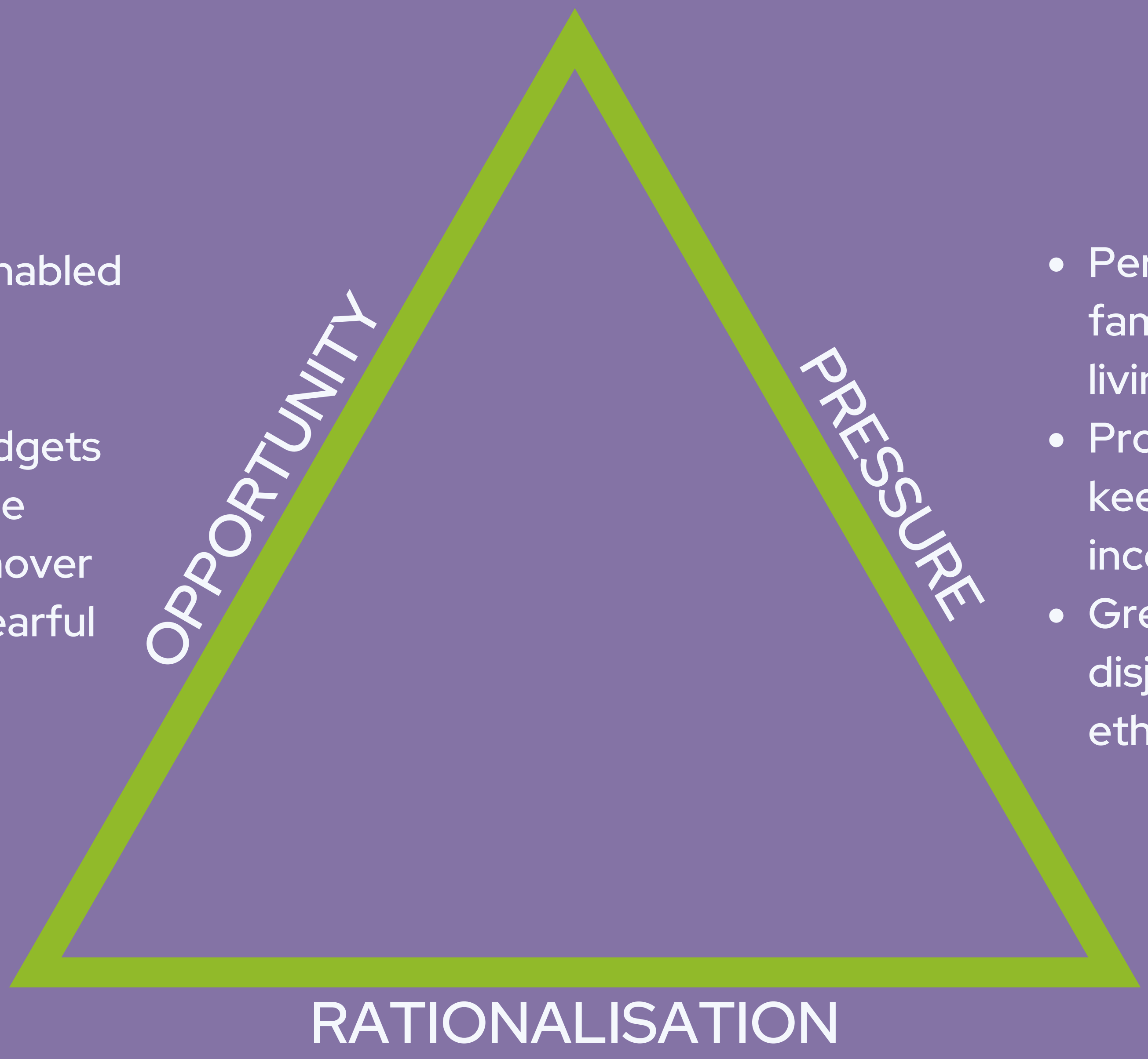
Fraud is a silent killer of businesses, eroding trust, draining resources, and leaving devastation in its wake. Yet many companies remain woefully unprepared, caught in a web of complex regulations and ever-evolving threats. The UK's Economic Crime and Corporate Transparency Act 2023 raises the stakes even higher, demanding robust fraud prevention measures from mid-caps up.

But here's the truth: most fraud risk assessments are dry, disconnected exercises that gather dust on shelves. They fail to capture the dynamic nature of economic crime and leave companies vulnerable to both legal and financial peril.

What if there was a better way? A method to transform fraud risk management from a compliance burden into a strategic advantage?

There is. We've developed a cutting-edge risk assessment tool that aligns fraud prevention with your company's core objectives (being successful).

- A.I. and tech-enabled scams
- Squeeze on compliance budgets
- Remote/flexible work, staff turnover
- People more fearful of speaking up



- Personal (debts, bills, family issues, cost of living, etc.)
- Professional (want to keep job, increase income, etc.)
- Greed (incentives disjointed from ethics)

- Cynicism (they don't care, going to fire me, etc.)
- Necessity (take care of self and others)
- Everyone else is (ethical fading and moral offsetting)

1. Definition of fraud

ethicsinsight

The UK Economic Crime and Corporate Transparency Act 2023 outlines various fraud offences, particularly within Schedules 11 and 13 of the Act. Companies must understand these offences to ensure compliance and effective prevention frameworks. Here are the main categories and definitions of fraud captured in the Act:

1. Fraud by False Representation
Definition: When a person dishonestly makes a false representation, intending to gain for themselves or another, cause loss to another, or expose another to a risk of loss.
Example: Providing false information on financial statements to secure loans or investments.

2. Fraud by Failing to Disclose Information
Definition: When a person dishonestly fails to disclose information that they are legally obligated to reveal to make a gain or cause a loss.
Example: Withholding information about a company's financial liabilities when seeking investment or credit.

3. Fraud by Abuse of Position
Definition: When a person in a position of trust abuses that position to make a gain for themselves or another dishonestly or to cause loss or risk of loss to another.
Example: Employees with access to company funds use their position to siphon money into their accounts.

4. Obtaining Services Dishonestly
Definition: Obtaining services for oneself or another through dishonesty, knowing that the services were being provided using false pretences.
Example: Using falsified documents to access premium services or memberships without paying.

5. Possession of Articles for Use in Fraud
Definition: Possession or control of any articles intended for use during or in connection with fraud.
Example: Holding fake identification documents or counterfeit credit cards intended to be used for fraudulent activities.

6. Making or Supplying Articles for Use in Fraud
Definition: Making, adapting, supplying, or offering to supply any articles with the knowledge that they are intended to be used to commit or assist in the commission of fraud.
Example: Manufacturing or distributing devices designed to skim credit card information.

7. False Accounting
Definition: This offence involves dishonestly destroying, defacing, concealing, or falsifying any account, record, or document required for an accounting purpose.
Example: Altering financial records to hide embezzlement or inflate profits.

8. Participation in a Fraudulent Business
Definition: Engaging in business or company activities to defraud creditors or other persons.
Example: Setting up shell companies to launder money or evade taxes.

1. Definition of fraud (cont.)

ethicsinsight

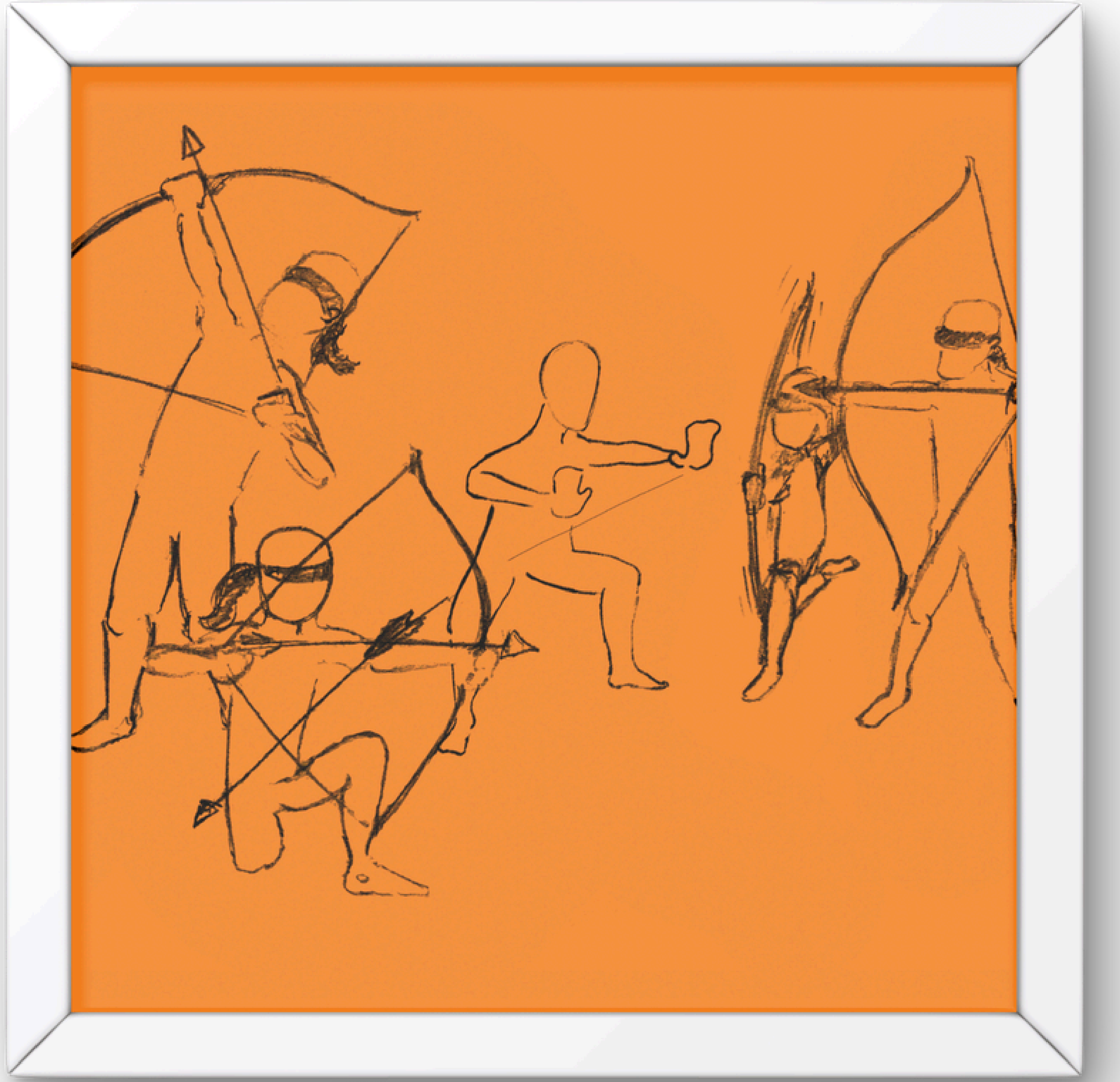
9. Conspiracy to Defraud
Definition: An agreement between two or more persons to carry out a plan to defraud others.
Example: Collaborating with others to create a Ponzi scheme.

10. False Statements by Company Directors
Definition: This offence occurs when a company director knowingly makes a materially false statement or misleading omission in a document relating to the company's affairs.
Example: A director deliberately understates the company's liabilities in financial reports to attract investors or secure loans.

11. Fraudulent Trading
Definition: Carrying on a business intending to defraud creditors or for any other fraudulent purpose, typically when a company continues to trade despite knowing it cannot pay its debts.
Example: A company director continuing to accept customer payments for goods or services while knowing the company is insolvent and unable to fulfil orders.

12. Cheating the Public Revenue
Definition: Engaging in any fraudulent activity that results in the loss of public funds or revenue, typically involving tax evasion or false claims for government benefits.
Example: A business deliberately underreporting its income to reduce tax liability, or an individual falsely claiming unemployment benefits while working.

These definitions provide a framework for identifying and categorising various fraudulent activities under the Act. By understanding these categories, companies can better develop strategies and policies to prevent, detect, and respond to fraud, ensuring they comply with the UK Economic Crime and Corporate Transparency Act 2023.



2. Who is covered?

ethicsinsight

The Act applies to large companies (and their subsidiaries) and partnerships. Additionally, large not-for-profit organisations, such as charities and incorporated public bodies, will fall within the scope. The offence will apply across all sectors.

Two of the three criteria below must be met for the ‘failure to prevent fraud’ offence to apply to an organisation:

- More than 250 employees
- More than £36 million turnover
- More than £18 million in total assets

The offence will also apply to parent companies of a group which meets at least two of the following criteria in the final year preceding the year in which the offence is committed:

- More than 250 aggregate employees
- An aggregate turnover of over £36 million net (or £43.2 million gross)
- An aggregate balance sheet of over £18 million net (or £21.6 million gross)

Companies will be held liable where an ‘associated person’ of a large company/partnership commits one of the fraud offences. The meaning of ‘associated person’ is broad and will include

- an employee, agent or subsidiary of the relevant organisation;
- an employee of a subsidiary and
- a person who otherwise performs services for or on behalf of an organisation.

Liability can attach to a parent company where a subsidiary’s employee committed a fraud offence for the benefit of the parent company and the parent company did not take ‘reasonable’ steps to prevent it.

Extra-territorial reach

While the Act itself is silent on the extra-territorial jurisdictional reach of the new offence, the government’s factsheet states that ‘if an employee commits fraud under UK law, or targeting UK victims, their employer could be prosecuted, even if the organisation (and the employee) are based overseas.’

An interpretation of this could be that where a large company based outside of the UK has an employee who commits a fraud offence under UK law or targets UK victims for the company’s benefit, that company may be liable under the ‘failure to prevent fraud’ offence.

Available defences

The Act provides a defence to the ‘failure to prevent fraud’ offence if an organisation can demonstrate that it had ‘reasonable procedures’ to prevent fraud.

The UK government will publish guidance about what constitutes ‘reasonable procedures’ before the new offence comes into force. Once released, this guidance should help companies determine whether their current fraud prevention mechanisms are sufficient or require enhancement.

Scorecard questions & indicators of best practice

Risk Assessment Questions & Considerations

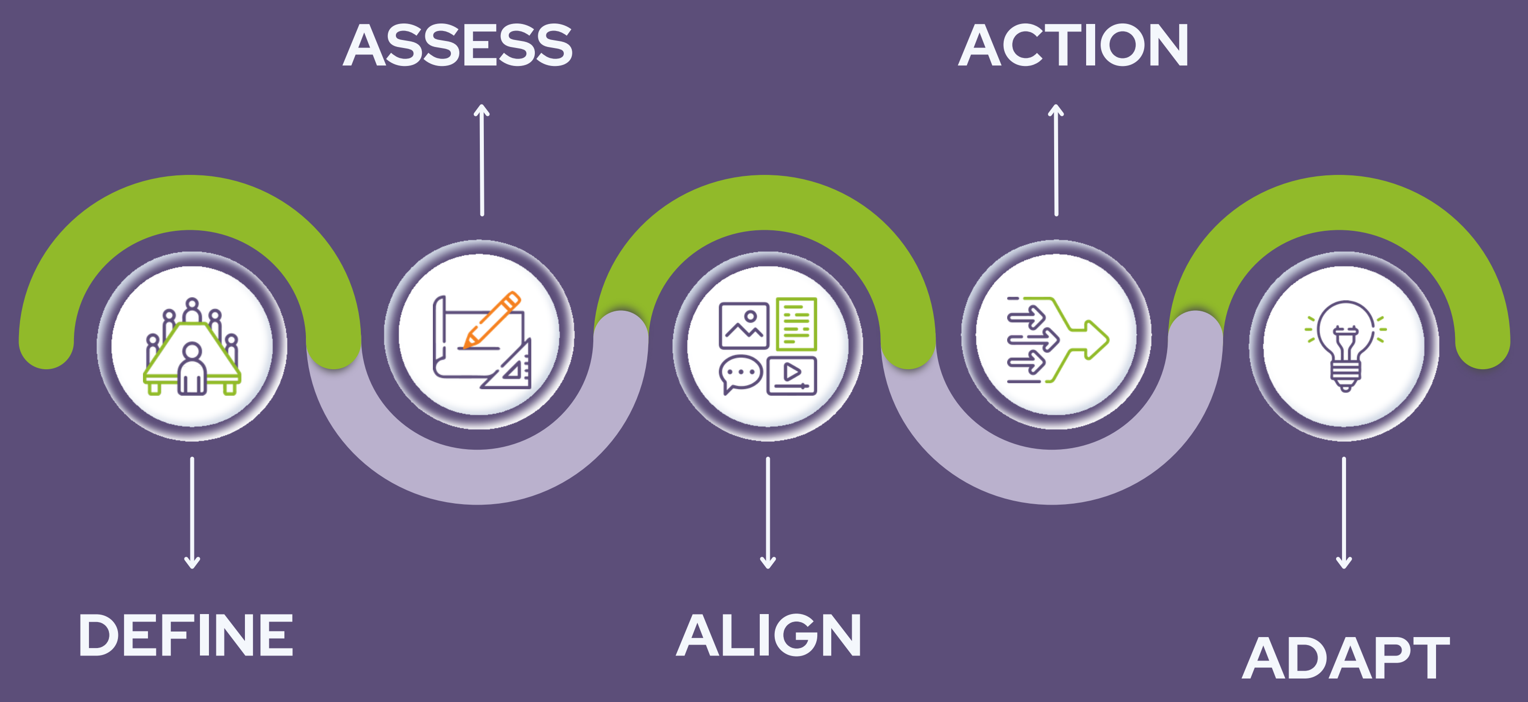
This comprehensive set of questions covers critical elements of a robust fraud risk management program in alignment with the UK Economic Crime and Corporate Transparency Act 2023.

The binary, scale, and multiple choice response options allow organisations to self-assess their current state and identify areas for improvement.

We include the questions below as we understand you may wish to include them in your existing risk assessment framework(s).

When you identify areas with gaps, you consider following up with additional open-ended questions that can also be included to gather more qualitative insights.

ethicsinsight



Section 1: Governance and Leadership

ethicsinsight

Questions

1. Is there a designated Chief Compliance Officer or equivalent role responsible for overseeing economic crime and fraud prevention? (Yes/No)
2. Does your board have a committee that oversees fraud risk management? (Yes/No)
3. How frequently does the board receive reporting on fraud risks and incidents? (Never, Annually, Quarterly, Monthly)
4. Are fraud risk management responsibilities integrated into senior executive performance evaluations? (Yes/No/Partially)
5. Do the board and senior management set an appropriate "tone at the top," emphasising ethical conduct and fraud prevention? (5-point scale)

Indicators of best practice

- The presence of a board-level committee focused on economic crime and fraud prevention.
- Regular reporting and updates to the board on economic crime, fraud risks, and incidents.
- Regular board-level discussions on emerging economic crime trends and their potential impact on the organisation.
- Clear escalation procedures for significant fraud risks or incidents to the board.
- Unrestricted access for internal audit to the board/audit committee.
- Mechanisms for employees to report concerns directly to the board.
- Document the board meeting minutes discussing economic crime and fraud prevention.
- Specific individuals or roles assigned responsibility for overseeing the implementation and effectiveness of fraud prevention measures.
- Integration of economic crime prevention responsibilities into performance evaluations and incentives for senior management.
- The board and CEO lead by example through their actions and communications.
- Documented responsibilities of board members related to fraud oversight.

Section 2: Policies and Procedures

ethicsinsight

Questions

1. Does the company have comprehensive policies addressing economic crime and fraud prevention covering all key risk areas? (Yes/No)
2. Do your policies clearly define the organisation's risk tolerance for fraud and economic crime? (Yes/No)
3. Rate the effectiveness of communication and implementation of anti-fraud policies across the organisation. (5-point scale)
4. Are regular assessments conducted to ensure policies are being followed? (Yes/No)

Indicators of best practice

- Written policies covering anti-fraud measures, anti-money laundering (AML, where relevant), anti-bribery, and corruption.
- Regular updates and reviews of policies to ensure they reflect current laws and best practices.
- Integration of fraud prevention policies into operational procedures and workflows.
- Regular benchmarking of policies against industry standards and regulatory expectations.
- Accessibility of policies to all employees through an intranet or other internal communication channels.
- Regular assessments or audits to ensure policies are being followed correctly.
- Articulation of acceptable risk levels in the fraud risk management policy.
- Alignment of risk tolerance with overall organisational risk appetite

Section 3: Risk Assessment and Management

ethicsinsight

Questions

1. Has the company conducted a thorough risk assessment to identify potential economic crime and fraud areas? (Yes/No)
2. Rate the robustness of your fraud risk identification process. (5-point scale: Weak to Robust)
3. When was your organisation's last comprehensive fraud risk assessment? (Within one year, 1-2 years, 2-3 years, Over three years)
4. Does the company conduct scenario analysis to assess the potential impact of fraud risks? (Yes/No/Partially)
5. Are data analytics and monitoring tools used to identify red flags or fraud indicators? (Yes/No/Partially)
6. How would you rate the effectiveness of strategies to mitigate identified fraud risks? (5-point scale)
7. Are roles and responsibilities assigned for fraud risk management? (Yes/No/Partially)

Indicators of best practice

- Comprehensive risk assessments covering various economic crimes, including fraud, money laundering, and bribery.
- Integration of fraud risk assessments into new product development and market entry processes.
- Data analytics and other tools identify potential red flags, anomalies, and emerging risk patterns (e.g., predictive fraud risk modelling).
- Implement internal controls and checks to prevent fraud and other economic crimes.
- Regular updates to risk mitigation strategies based on new threats or incidents.
- Designated executive-level owner for overall fraud risk management.
- Documented roles at all levels for implementation and oversight.
- Integration into performance goals and incentives.
- Processes to identify new fraud typologies and schemes.
- Periodic updates to risk assessments based on new threats.

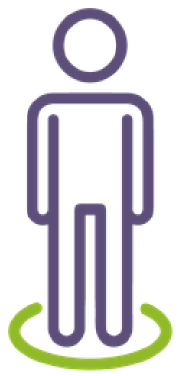
Section 4: Detection and Response

Questions

1. Are there effective mechanisms to detect economic crime and fraud? (5-point scale)
2. Are there real-time mechanisms to monitor and audit high-risk transactions? (Yes/No/Partially)
3. Does the company have a clear and compelling response plan for economic crime and fraud incidents? (Yes/No)
4. Are there robust procedures for investigating suspected fraud incidents? (Yes/No/Partially)
5. Are there consistent disciplinary actions for substantiated fraud cases? (5-point scale)
6. Rate the effectiveness of your fraud detection mechanisms (e.g. data monitoring, whistleblower hotline). (5-point scale)
7. Rate the effectiveness of your controls to prevent cyber-enabled fraud (e.g. phishing, malware). (5-point scale)
8. Are there mechanisms to detect and respond to data breaches or network intrusions? (Yes/No/Partially)
9. Are there robust processes for segregating duties and managing conflicts of interest? (Yes/No/Partially)
10. How frequently are targeted fraud audits conducted? (Never, Annually, Every six months, More frequently)
11. Is there a documented incident response plan for detected fraud cases? (Yes/No)
12. Does the company have a process for conducting post-incident reviews to improve fraud detection and response? (Yes/No)
13. Do you conduct comprehensive due diligence on third parties before onboarding? (Yes/No/Partially)
14. Rate the robustness of your third-party monitoring processes. (5-point scale)
15. Are there mechanisms to ensure third parties comply with your anti-fraud policies? (Yes/No/Partially)
16. How frequently are third-party relationships re-assessed for fraud risk? (Never, Annually, Every six months, More frequently)

Indicators of best practice

- Monitoring systems and software are used to detect suspicious activities.
- Encouragement of whistleblowing through anonymous reporting channels.
- Regular audits and forensic investigations to uncover potential fraud.
- Documented incident response plan outlining steps to be taken when economic crime or fraud is detected.
- Establishment of a dedicated fraud investigation unit with specialised skills.
- Regular testing of the incident response plan through tabletop exercises or simulations.
- Implementation of continuous monitoring systems for high-risk areas.
- Coordination with law enforcement and regulatory bodies as required.
- Defined protocols for escalating and reviewing allegations.
- Skilled investigators trained in forensics and evidence handling.
- Procedures for root cause analysis and remediation.
- Documented disciplinary policies and consequences.
- Equitable application regardless of employee position or level.
- Communication of disciplinary actions as a deterrent.



Section 5: Continuous Improvement

Questions

1. Does the company regularly monitor and review its economic crime and fraud prevention framework? (Yes/No)
2. How often is your fraud risk management framework reviewed and updated? (Never, Annually, Every six months, More frequently)
3. Are feedback mechanisms in place to identify areas for improving fraud controls? (Yes/No)
4. Is there a formal process for incorporating lessons learned from industry peers or regulatory actions into the fraud risk management framework? (Yes/No)
5. Rate your organisation's ability to adapt fraud prevention measures to new threats. (5-point scale)
6. Is there a process to analyse root causes and remediate control gaps after fraud incidents? (Yes/No/Partially)
7. Are external parties leveraged to validate and enhance the fraud program? (Yes/No/Partially)

Indicators of best practice

- Periodic reviews and updates to the framework based on feedback and changes in the regulatory environment.
- Participation in industry forums or working groups focused on economic crime prevention.
- Regular assessment of the organisation's fraud risk management maturity against recognised frameworks.
- Regular internal audits to assess the effectiveness of the framework.
- KPIs are used to measure the success of fraud prevention measures.
- Designated senior executive responsible for program oversight.
- Engagement of external advisors or subject matter experts.
- Benchmarking against industry best practices.
- Incorporation of regulator feedback and guidance.

Section 6: Reporting and Whistleblowing

Questions

1. Is there an anonymous whistleblowing mechanism for employees to report suspected fraud? (Yes/No)
2. How would you rate the effectiveness of your whistleblowing program? (5-point scale)
3. Are there metrics in place to measure the effectiveness and utilisation of the whistleblowing program? (Yes/No)
4. Are there clear protocols for escalating and investigating whistleblower allegations? (Yes/No/Partially)
5. Is there protection against retaliation for whistleblowers reporting in good faith? (Yes/No)

Indicators of best practice

- Documented channels and protocols for reporting violations.
- Mechanisms to ensure confidentiality and prevent retaliation.
- Explanation of whistleblower process in fraud risk management policy.
- Regular communication with employees about the outcomes of whistleblowing reports (while maintaining confidentiality).
- Periodic independent review of the whistleblowing program's effectiveness.

Section 7: Employee Training and Awareness

Questions

1. Are employees regularly trained and made aware of economic crime and fraud prevention measures? (5-point scale)
2. Is there role- or function-specific fraud prevention training for employees in high-risk positions? (Yes/No)
3. Is there a process to assess employees' understanding and retention of fraud prevention training? (Yes/No)
4. Rate the effectiveness of your employee screening and due diligence processes. (5-point scale)
5. How frequently are employees provided fraud awareness and ethics training? (Never, Annually, Every six months, More frequently)
6. Rate the quality and comprehensiveness of fraud training programs. (5-point scale: Poor to Excellent)

Indicators of best practice

- Training programs for employees on economic crime and fraud prevention policies.
- Ongoing training programs for new and existing employees.
- Awareness campaigns should keep economic crime and fraud prevention at the forefront of people's minds.
- Evaluation of training effectiveness through assessments and feedback.
- Incorporation of real-world case studies and scenarios in fraud awareness training.
- Implementation of a fraud prevention certification program for key employees.
- Use of gamification or interactive elements in fraud awareness training to increase engagement.

Assessing your score

All questions are assessed on a 5-point scale to keep answers equally weighted, as follows:

- Yes (5 points), No (0) points
- Yes (5 points), Partially (3 points), No (0 points)
- Scale responses (0-5 points)
- Never (0 points), Annually (2 points), Quarterly (4 points), Monthly (5 points)
- Within one year (5 points), 1-2 years (3 points), 2-3 years (2 points), Over three years (0 points)

There are 50 questions in total. The maximum possible score is 250 points. If you convert your score into a percentage and compare it to the adjacent 👉 table, you can benchmark your result against best practices.

Beyond scores, the general idea is to identify potential gaps and priorities, which you can review and decide if they're appropriate for your organisation. If you'd like to go through your scores, you can set up a call with me, here.

ethicsinsight

Score	Risk Rating
<40%	Low preparedness to manage fraud risks, and weak compliance with best practice
41%-79%	Moderate preparedness to manage fraud, likely with some strong performing areas, focus on gaps to ensure compliance with best practice
>79%	Strong fraud risk management and robust compliance with the requirements of best practice

Who we are and how we work

Our Experience

Some of the great people we work with:

ERICSSON
EVBOX
TI Fluid Systems
CSL Behring
Biotherapies for Life™
ACFE
Association of Certified Fraud Examiners
Swedfund
ADB
ASIAN DEVELOPMENT BANK
TRANSPARENCY INTERNATIONAL
the global coalition against corruption
FFIEC
Genmab
Association of Corporate Investigators
wsp

What they say about us:

“Rupert's fresh approach, flexibility, experience, creativity and professionalism made him an outstanding partner. On a scale of 1-10, I rate Ethics Insight as a 10."

Rory Donaldson, Business Integrity Programme Manager – Transparency International

"Rupert is particularly skilled at sensitively engaging with firm leadership on very tricky topics. He helps our investments become better businesses."

Rita Roca, Business Integrity Leader, Impact Fund Denmark

"Ethics Insight provides a toolkit to operationalise an organisation's ethics, fraud risks and compliance. They help build a culture where doing the right thing is the norm."

Kevin Withane, Founder of Diversity X and UKBAA Angel Investment Award Winner 2023

RUPERT EVILL

Rupert has 25 years of experience managing risks, ethics, compliance, and crises across more than 30 sectors and 80+ countries. Before founding Ethics Insight, he worked in roles focused on investigations, due diligence, risk analysis, crisis response, and Ethics & Compliance (E&C) advisory support.

He has augmented this professional experience with postgraduate qualifications in Business Sustainability Management, ESG impact, and Behavioural Analysis and Investigative Interviewing. He is a Certified Fraud Examiner (and sit on the ACFE's Fraud Examiner Job Analysis Task Force) and also sit on the advisory panel of the Association of Corporate Investigators. Rupert is the author of Bootstrapping Ethics, Integrity Risk Management for Real World Application.

Rupert uses this training and frontline experience – having seen what works and what doesn't – to inform practical and effective guidance to help organisations make better and more sustainable (fraud) risk frameworks.

Examples of Rupert's recent experience include:

- Risk assessment, gap analysis, and (fraud) risk program implementation projects across 20+ organisations in the past year, in sectors including: renewables, financial services, consumer goods, agriculture, manufacturing, and infrastructure.
- Investigations into corruption, anti-competitive practices, and fraud across 50 donor- or investor-led infrastructure projects, including energy and renewables, across 22 countries in the past 4 years.
- Conducting business integrity risk assessment and benchmarking programs across 20+ organisations in 35+ countries using the Ethics Insight Assessments, typically saving 40%-50% of projected costs.
- Developed and/or delivered training for 32,000+ people in areas including fraud prevention (regular speaker at ACFE and broader industry events), behavioural analysis, risk assessment, investigations, and crisis management.

Book a call (click or scan the QR code)

ethicsinsight