IGNE – COUNTER FRAUD STRATEGY

1.0 PREFACE

This document details the anti-fraud strategy for Igne (henceforth referred to as "the Group"). This strategy is crafted to safeguard the Group, its employees, and all associated parties from any fraudulent actions and activities.

The fundamental ethos of the Group is rooted in transparency and ethical commercial trading. This strategy is an extension of that ethos, aiming to encourage a culture wherein honesty, integrity, and a strong stance against fraud are paramount to all commercial and financial activities.

The counter fraud strategy document is for employees of Igne Group Limited and all subsidiaries. The Igne Group Limited Companies Comprise of Igne UXO Limited, W.B. and A.D. Morgan Ltd, Raeburn Drilling & Geotechnical Ltd, Allied Exploration & Geotechnics Ltd, DTS Raeburn Ltd and Terra Tek Ltd.

2.0 CLARIFYING FRAUD

Within the context of this strategy, "fraud" is characterized as deliberate deception, misrepresentation, or the withholding of truths with the intention of personal enrichment or inflicting financial loss on another party. The Fraud Act 2006 defines fraud as the intention to obtain a gain for oneself or for another, or to cause or expose another to the risk of a loss.

The Fraud Act 2006 covers the following offences:

- Dishonestly making an untrue or misleading representation
- Dishonestly failing to disclose information which one is legally bound to disclose
- Dishonestly abusing a position of trust, in which they are expected to safeguard, or not to act against, the financial interests of others.
- Failing to prevent tax evasion.

All cases of suspected fraud, or attempted fraud, will be thoroughly and promptly investigated.

What is not acceptable:

It is not acceptable for any employees within the Group or anyone on their behalf to commit:

A) **Abuse of position** – Using the position in the Group to commit fraud, e.g. syphoning off finances for personal gain.
B) **Fraud** – By assisting organised crime.
C) **Bid rigging** – Bid rigging occurs when bidders agree among themselves to eliminate competition in the procurement process – thereby denying a fair price.
D) **Charity fraud** – Skimming of collection boxes, theft of inventory / donated items
E) **Cheque fraud** – Forged cheques, counterfeit cheques, fraudulently altered cheques
F) **Insurance fraud** – Knowingly submitting false, multiple or exaggerated insurance claims or the deliberate destruction of items or property in order to claim on insurance
G) **License Fraud** – Not paying for licences by concealing activities
H) **Staged/induced motor vehicle accident fraud**
I) **Motor finance fraud** – Giving incomplete or inaccurate information to a lender, conversion fraud (selling a vehicle with outstanding finance) and first party fraud (paying fraudulently).
J) **Payroll fraud** – Payroll fraud can occur when unauthorised changes are made to payroll systems, such as the creation of false payroll records or unauthorised amendments such as changes to salary payments or allowances.

K) **Recruitment fraud** – Occurs when false information is provided in order to gain employment, for example by lying about employment history and qualifications or providing false identification documents (e.g. false documentation demonstrating the right to work in the UK).

L) **Procurement fraud** – Procurement fraud is any fraud relating to the purchasing of goods and services. It covers the entire procure-to-pay lifecycle, including fraud in the tender / bidder selection and contract award stages (e.g. illicit cartel activity or bribery of an official to influence the tendering process); as well as fraud occurring during the life of the contract (e.g. false, duplicate or double invoicing). Procurement fraud can occur with or without the collusion of an employee within an organisation (sometimes referred to as an "insider").

M) **Tax Evasion** – deliberately omit, conceal or misrepresent information in order to reduce their tax liabilities.

3.0 GOALS

The salient goals of this strategy are as follows:

- To identify and prevent fraud within the Group.
- To thoroughly probe and investigate instances of fraud when they occur.
- To ensure suitable actions, including disciplinary measures, are taken against those found guilty of committing fraud.
- To minimize the financial and reputational damage due to fraudulent activities.
- To cultivate a culture that values honesty and ethical behaviour

4.0 DUTIES AND RESPONSIBILITIES

All members of staff and stakeholders share the responsibility to protect the Group's resources and promptly report any suspicions or evidence of fraudulent activities, and therefore the prevention, detection and reporting of fraud is a responsibility shared amongst all those working for the Group or within the Group's control. All workers are required to avoid any activities that might lead to, or suggest, fraudulent activities.

The ultimate accountability for fraud prevention, detection, and the successful execution of this strategy lies with the board of directors within Igne.

Counter Fraud Champions

Our nominated Counter Fraud Champions are:
Paul Breslin – ESG and Regulatory Risk Director
Sarah Murphy –
Craig Scandrett – Group Financial Controller

The Role of the Igne Nominated Counter Fraud Champions (CFC) is crucial in promoting and maintaining a robust anti-fraud culture. This individual shall act as the focal point for fraud prevention and detection efforts, working in coordination with all departments within the Igne Group of Companies. The following constitute the key duties and responsibilities of the Counter Fraud Champion:

1. **Awareness and Training**: Ensure that fraud awareness training is in place to educate employees about different types of fraud, their impact and prevention measures. Training is designed to enhance the employees' understanding of fraud risks, red flags and reporting mechanisms. Oversee the dissemination and understanding of anti-fraud policies throughout the organisation.
2. **Policy development and Implementation**: Collaborate with all Igne departments including HR and Finance to develop comprehensive anti-fraud policies, procedures and controls.
3. **Risk Assessment and Mitigation**: Conduct regular fraud risk assessments to identify vulnerabilities, potential fraud schemes and areas requiring enhanced controls, as well as development of the fraud prevention strategy and any control measures. They will also be responsible for monitoring the

effectiveness of these controls and proposing recommendations.

4. **Reporting and investigation**: Establish and maintain a confidential reporting mechanism (including a whistleblower channel) to enable employees to report suspected fraudulent activities. Ensure that reported incidents are promptly and thoroughly investigated, either independently or in coordination with appropriate departments and external resources. Liaise with legal counsel and law enforcement where required to facilitate investigations and legal proceedings.
5. **Collaboration and Communication**: Foster a culture of collaboration with all relevant departments, to ensure a coordinated approach to fraud prevention and response. Communicate regularly with senior management and the Board of Directors to provide updates on fraud prevention initiatives, emerging risks, and the effectiveness of anti-fraud measures.
6. **Monitoring and Compliance**: Establish mechanisms for ongoing monitoring of potential fraud indicators, such as data analytics (where applicable), internal audits and reviews. Monitor compliance with anti-fraud policies and procedures, investigate potential breaches and recommending disciplinary actions, where necessary.

5.0 AVOIDING FRAUD

To prevent the occurrence of fraud, the Group will:

- Establish stringent internal controls and schedule regular evaluations. These include (but are not limited to) segregation of duties, access restrictions to both electronic and hard copy information, dual authority and two factor authentication on bank accounts.
- A thorough delegated authorities matrix, which is enforced through the financial system with automated approval limits as described below.
- Provide comprehensive training and awareness sessions to staff about the risks of fraud and methods to prevent it. This training is mandatory for all employees upon commencement of employment and every 2 years thereafter.
- Encourage a clear code of conduct and ethics policy for all employees.
- A policy of verbal referral with a known contact for change in client / supplier banking details.
- Set up a confidential mechanism for reporting (whistleblowing) to ensure anonymous and safe reporting.

Furthermore, the Group shall undertake compliance checks to minimise its exposure to the risk of fraud. In order to ensure this is implemented, Igne shall undertake due diligence checks as follows:

New Customers, Vendors or Suppliers

A. At enquiry stage, undertake a Credit Check using Experian services for contracts over £10,000 value
   i. If the results of the credit check are satisfactory then the customer is accepted by the relevant business and the BU lead will authorize continuation of the bid.
   ii. If the results have issues raised, then the BU Lead reviews the report to determine if we continue with the business. This would escalate to the CFO if the value was of significant value.

New Workers

A. Verify competencies to ensure they are suitable for the role
B. Verify Right to Work in the UK
C. Verify References
D. Complete a Compliance Check using the approved checking provider.
E. Check driving license (if required)

In addition to the above, no new clients, suppliers or subcontractors are to be added to any of the Company's systems without having first been screened and verified with this compliance process. Copies of the outcome of the process are to be retained for future reference.

Authority Matrix
To ensure that significant decisions, payments, contracts, and agreements are only made by senior management. This authority matrix is available to all workers and is enforced by senior management and the finance department.

The matrix covers the limitations of managers, directors, the CEO and CFO including;

- Project expenditure
- Personnel
- Binding Agreements
- Opening and closing of bank accounts
- Overseas travel
- Joint Ventures – CEO and CFO Only
- Sale and Disposal of Assets – CEO and CFO Only
- Expenses
- Donations - All donations must be signed off by 2 directors

Any employee who breaches the authority matrix may face disciplinary action, which could result in summary dismissal for gross misconduct.

6.0 IDENTIFYING FRAUD

The Company will detect fraudulent activities through:

- Frequent internal and external audits
- Annual audit of statutory accounts
- Regular checks and monitoring of financial and operational systems
- Effective mechanisms for reporting, escalating, and addressing potential fraud.
- Regular board meetings where operational issues, problems and evaluations are discussed.

Internal Audit Team and Internal Audits

The internal audit team responsible for fraud detection within the Group shall consist of employees with expertise in industry. This independent function shall report directly to the board of directors, ensuring objectivity and minimizing conflicts of interest. The team's main duties include conducting and reviewing risk assessments, developing anti-fraud policies and procedures, fostering whistleblowing mechanisms, conducting continuous monitoring and auditing and collaborating with external parties such as law enforcement agencies and forensic accounting firms, where required.

The Internal audits shall focus on the following processes:

- Fraud risk assessment, focusing on company-specific risks (e.g. bid rigging, improper billing, false claims, collusion with subcontractors).
- Evaluation of internal controls and compliance with anti-fraud policies and procedures.
- Financial transactions, expense reporting, and procurement practices.
- Vendor management processes and conflict of interest prevention.
- Project tracking and cost management.
- Ongoing monitoring and auditing of key risk areas.
- Investigation of reported incidents and suspected fraud.
- Continuous improvement of internal audit procedures.

An internal Counter Fraud Compliance Audit shall be conducted annually.

Guidance for identification and prevention of Fraud for Company employees

The following constitute some of the primary factors and principles that must be followed to ensure identification and prevention of fraud for all employees and shall be re-iterated as part of the awareness and training programme:

Do we know who we are dealing with?

Are they a known customer? Even if the client is known also consider whether the specific staff member a known entity too? if there is an intermediary do we have contact with the end client and can contact be made directly where required?

Never take things at face value.

Is the sender real? Do we know who they are? Why are they contacting the Company? is their reason for contacting you legitimate? Does it seem like their normal communication? Does it 'feel' right and should scepticism be applied?

Are you being asked to do something unusual or its purpose unclear?

Are any weblinks that are highlighted genuine? Are you being told to download software? Are you being put under time pressure to make a quick decision?

Get confirmation of new details or of a change to existing details

Make sure that any request is genuine; don't accept bank details (or a change of bank details) without getting additional confirmation; pick up the phone and speak to the client; is there an alternate contact you can use for confirmation? If the request is genuine are the new details correct?

Do not be afraid to raise your suspicions.

If you are not sure then say something; talk to a colleague or your line manager; chat through your concerns; make sure you are happy before proceeding.

7.0 RESPONDING TO FRAUD

When fraud is detected within the Igne Group of Companies, it is crucial to respond with an appropriate level of investigation to determine the extent of the fraud, identify the individuals involved, and take appropriate legal and disciplinary actions. The Group shall therefore follow the below steps when responding to Fraud:

1. **Secure Evidence**: All relevant evidence related to the suspected fraud must be preserved. This includes financial records, emails, documents, transactional data, and any other information relevant to the investigation. The Counter Fraud Champion must ensure that the evidence is secured and protected from tampering. In the case of a conflict of interest which involves the Counter Fraud Champion, this information shall be collated and secured by a senior member of staff – directly appointed by the CEO.
2. **Assemble the Investigation Team**: Top level management led by the CEO must form an internal investigation team comprising individuals with expertise in internal controls, forensic accounting and knowledge of legal matters (including any external consultancy if required). This team should be independent and free from any conflicts of interest with the parties involved. The Counter Fraud Champion should form part of this team, unless excluded due to conflicts of interest.
3. **Establish a Plan**: Develop a detailed investigation plan outlining objectives, scope and methodology of the investigation. Identify potential risks, key areas to focus on, and the timeline of the investigation.
4. **Conduct interviews**: Interview relevant employees, including executives, managers, and staff members who could have knowledge of the fraudulent activities. Conduct the interviews in a confidential and unbiased manner, ensuring that proper documentation and records are maintained.
5. **Engage external experts**: If necessary, seek assistance from external experts such as forensic accountants and legal advisors with experience in financial fraud.

6. **Analyse financial records**: Scrutinise financial statements, bank records, invoices and other financial documents to identify any irregularities, discrepancies or fraudulent transactions. Look for patterns, unusual transactions, or unauthorized access to accounts.
7. **Review internal controls**: Evaluate the effectiveness of internal controls and identify any weaknesses or gaps that may have contributed to the fraud. Assess the adequacy of segregation of duties, approval processes, and access controls.
8. **Assess compliance with Laws and Regulations**: Determine if any laws or regulations have been violated and assess the potential legal implications. Consult legal counsel to understand the legal obligations and potential consequences for the Company and individuals involved.
9. **Report Findings**: Prepare a comprehensive report detailing the findings of the investigation, including the nature and extent of the fraud, individuals involved, and any recommendations for remedial actions. The report should be shared with the board of directors, CEO, and any legal advisors.
10. **Take Appropriate Actions**: Based on the investigation findings, take appropriate actions to address the fraud. This may include disciplinary actions such as termination or suspension of implicated employees, recovery of funds, strengthening internal controls, and implementing preventive measures to mitigate the risk of future fraud.
11. **Cooperate with Authorities**: If the fraud involves criminal activities, cooperate fully with law enforcement agencies and regulatory authorities. Provide them with the necessary information, evidence, and support require for their investigation.

It is crucial that throughout the investigation process, confidentiality and objectivity are maintained, as well as compliance with all legal and ethical requirements. The Group must consider seeking guidance from legal advisors where appropriate to ensure compliance with applicable legislation at every stage of the investigation.

8.0 ASSESSING FRAUD RISK

Regular fraud risk assessments will be conducted by the Company to identify potential weak points and bolster controls accordingly. The fraud risk assessment shall be reviewed annually by the Counter Fraud Champion in liaison with the internal audit team and senior management at top level across all Companies of the Igne Group and will be revised in conjunction with the Counter Fraud Strategy. The Counter Fraud Risk Assessment for the running year shall be included as an appendix to this document.

9.0 EDUCATION AND AWARENESS

The Company will host regular sessions on training and awareness to ensure that the staff members are equipped with the necessary knowledge and skills to prevent and identify fraud. All new employees are also required to undertake online CPD accredited courses, with a refresher course undertaken every 2 years.

The Company promotes awareness of fraud through its staff induction process, ensuring that all employees understand their responsibilities in preventing, identifying, and reporting fraudulent activity. This includes mandatory awareness of, and compliance with Igne's Anti-Bribery and Corruption Policy.

All new employees are required to complete CPD-accredited training in Fraud Prevention and Anti-Bribery and Corruption, with refresher training undertaken every two years to maintain awareness and understanding.

10.0 REPORTING LINES FOR INTERNAL AND EXTERNAL STAKEHOLDERS

Internal Stakeholders

Our primary internal stakeholders include all employees and the Board of Directors.

1. Employees: All employees are required to immediately report any suspicion of fraudulent activity to their Line Manager or the Counter Fraud Champion. Employees can report anonymously, and all reports will be treated with utmost confidentiality and professionalism as per the Company's Whistleblowing Policy.

2. Line Managers: Line managers are responsible for reviewing and escalating reports of suspected fraud to the Counter Fraud Champion or another member of the internal audit team. They must ensure that any concerns raised by their team members are taken seriously and addressed promptly.

3. Counter Fraud Champions: The Counter Fraud Champions is responsible for conducting preliminary investigations into reports of suspected fraud. They will liaise directly with the CEO, providing regular updates and making recommendations for further actions. They will also be responsible for undertaking the annual Counter Fraud Compliance audit.

4. The CEO will receive updates from the Counter Fraud Champion, make decisions on any necessary investigations or disciplinary actions, and report significant issues to the Board of Directors.

5. Board of Directors: The Board will be informed of significant fraud risks or incidents, and will review and monitor the overall effectiveness of the Company's counter fraud strategy.

External Stakeholders

Igne encourages a culture of transparency and accountability, and as such, we welcome any reports or suspicions of fraudulent activity. We have outlined the recommended reporting procedures below for our external stakeholders, including Clients and members of the public.

1. Clients: Clients who suspect fraudulent activity should report their suspicions directly to their designated account manager or contact person at Igne. If for any reason they feel uncomfortable doing so, they are encouraged to use our general contact email address: hello@igne.com. Please mark the subject of your email as "Confidential: Fraud Report."

2. Members of the Public: Members of the public can report suspected fraudulent activity by sending an email to hello@igne.com. Please mark the subject of your email as "Confidential: Fraud Report." Additionally, they can send a letter to our Head Office, marking the envelope 'Private and Confidential – Fraud Report'.

All communication channels mentioned above are regularly monitored, and we ensure that every report received is taken seriously, treated with upmost confidentiality, and investigated thoroughly. Igne are committed to ensuring that no one suffers any detrimental treatment as a result of reporting their suspicion in good faith about fraudulent activities. Any instances of detrimental treatment related to a report of potential fraud should be reported immediately, and will be treated seriously.

11.0 STRATEGY EVALUATION

This anti-fraud strategy will undergo an annual review to ascertain its efficacy and any make necessary updates or improvements. Updates to this strategy shall be briefed to all Igne senior management (including

Business Unit Leads and Directors) during the Annual Quality Management Review Meeting who shall then be responsible for disseminating the information to all other members of staff within the Company.

12.0 CONFIDENTIALITY AND WHISTLEBLOWING

The Company holds a strong commitment towards ensuring that employees are able to report any suspicions or evidence of fraud without fearing any retaliation or negative consequences. A confidential whistleblowing policy is in place that provides protection to those who report suspected fraudulent activities.

13.0 CONCLUSION

Igne takes pride in maintaining the highest standards of transparency, integrity, and accountability. The company firmly believes that its organizational culture does not tolerate fraud and can maintain robust processes that act to prevent such malpractice. Igne is committed to fostering an environment where ethical behaviour is valued, and fraudulent activities are swiftly identified and handled effectively.

This document outlines the fundamental principles and practices that Igne will employ to prevent, detect, and respond to fraud. It serves as a guide to ensure that we maintain and uphold the highest standards of ethical conduct across all areas of our operations. Our commitment to this strategy reflects our dedication to maintaining integrity, trust, and confidence among our stakeholders, employees, clients, and the broader trading community

Reference:	PR037	**Title:**	Igne Counter Fraud Strategy		
Version:	1.2	**Date Issued:**	13/01/2025	**Review Date:**	Dec 2026
Document Owner:		ESG and Regulatory Risk Director			

Version	Last Updated	Details	Author	Approved By
1.0	Oct 2024	First Issue	K Tsiminis	R Hunter
1.1	Oct 2025	Updated to include Fraud Risk Assessment	K Tsiminis	R Hunter
1.2	Dec 2025	Updated to include Counter fraud Champions	P Breslin	R Hunter

.

Appendix 1 - Counter Fraud Risk Assessment – October 2025

Risk No.	Risk	Activity	S	L	RR	Mitigations	Responsibility	S	L	RR
1	Fake invoices or overbilling	The risk concerns the payment of invoices for goods or services that were never supplied or were overpriced. This could include fraudulent claims for materials, labour, or subcontractor fees.	4	2	8	- Verify every invoice against the contract and purchase order to ensure that the works were completed before payment is issued. - Conduct audits of invoices and payments - Implement a two-person approval process for large invoices - Train employees on how to identify fraudulent invoices	Accounts Payable department, with oversight from the CFO	4	1	4
2	Collusion between employees and vendors	The risk concerns the potential for employees to collude with vendors to overcharge for goods or services, or to receive kickbacks in exchange for awarding contracts. It could also include the use of fictitious vendors or shell companies to defraud the Company.	4	2	9	- Conduct background checks on vendors and their principals - Rotate employees who handle vendor relationships - Implement a vendor approval process that includes a due diligence review - Require competitive bidding for all contracts where possible	Procurement department	4	1	4
3	Theft of materials and equipment	The risk concerns the theft of construction materials and equipment from job sites (or local depots) or any other storage areas. It could also include the unauthorized use of company-owned equipment (including vehicles) by employees.	3	3	9	- Use of security cameras and alarms to deter theft. Applicable for all business unit offices as well as sites wherever possible. - Conduct regular inventory checks and reconcile them against purchase orders. - Implement a system to track equipment usage. - Train employees on how to identify and report suspicious activity (via iHASCO accredited courses)	Site management, with oversight from the Operations Manager (for sites. Business Unit Leads for each respective Igne facility	3	1	3
4	Falsification of timesheets and expense claims	The risk concerns the submission of fraudulent timesheets or expense claims by employees. This could include the overstatement of hours worked, or the submission of false receipts for expenses that were not incurred.	3	2	6	- Implement a system to track employee hours and location (vehicle trackers, daily diaries from supervisors for site, check in procedures for offices) - Require detailed expense reports with receipts - Conduct spot checks of timesheets	HR department, respective managers with oversight from the finance department	3	1	3
5	Bribery and corruption	This risk concerns the potential for employees or vendors to engage in corrupt practices, such as offering or accepting bribes in exchange for favorable treatment. This could include the payment of bribes to obtain contracts or permits, or the acceptance of gifts or entertainment that could compromise an employee's impartiality.	4	2	8	- Develop a code of conduct that prohibits bribery and corruption. - Conduct checks on all employees and vendors as per provisions in the main body of this document - Implement a system to track gifts and entertainment provided to employees. - Train employees on the Company's anti-bribery and corruption policies.	Respective managers, Business Unit Leads with oversight from HR and finance departments	4	1	4