Fraud Risk Management Policy

Version:	4
Effective from:	March 2024
Reviewed date:	2 years from the effective date
Expiry date:	March 2026

Contents

Introduction

The term fraud is commonly used to include activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. In a broad sense, fraud can include any crime where deception was involved. Fraud is defined by Black's Law Dictionary as:

"A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment"

Hargreaves Services plc and its subsidiary undertakings ("the Group") is faced with these risks and should be prepared to manage these risks and approach their potential impact in a professional manner.

A fraud committed against the Group could have the following impact:

- Actual financial loss;
- Damage to the reputation of the Group and our employees;
- Negative publicity;
- Additional costs and internal time incurred for investigative work and litigation;
- Potential loss of employees and customers;
- Damage to relationships with customers and suppliers;
- Impact on employee morale.

The Group remains committed to the deterrence, detection and correction of misconduct and dishonesty. The discovery, reporting and documentation of such acts will provide a foundation for the protection of innocent parties, support disciplinary action against offenders (up to and including dismissal where appropriate), referral to law enforcement agencies if required and the recovery of assets.

Aim of Policy

The purpose of this document is to set out the Group's policy regarding the deterrence, detection and investigation of fraud, including misconduct or suspected misconduct or dishonesty, by employees and others who interface with the Group. It is also to provide guidance regarding appropriate actions to take in the event of suspected acts arising.

Definition of Fraud

For the purposes of this policy, fraud, misconduct and dishonesty include, but are not limited to:

- Theft or other misappropriation of assets, including assets of the Group, our customers, suppliers or others with whom we have a business relationship;
- Misstatements and other irregularities within our company records, including the intentional misstatement of operational and financial results;
- Profiteering as a result of insider knowledge of the Group's activities;
- Disclosing confidential or proprietary information to outside parties;
- Forgery or other alteration of documents;
- Accepting or seeking anything of value from customers, suppliers or other persons providing services to the Group;
- Unlawful acts.

Responsibilities

Overall responsibility for the Risk Management policy of the Group sits with the Board. This includes the approval of this Fraud Risk Management policy and ensuring that sufficient safeguards and frameworks are in place to allow for the effective detection and prevention of fraud. The Board is also required to approve the level of fraud risk appetite proposed by the Business Unit Managing Directors.

The Board may delegate the task of implementing this framework to the Business Unit Managing Directors, who will have effective day to day responsibility for:

- Proposing a suitable level of risk appetite in relation to fraud risk;
- Ensuring employees within their business unit are adequately briefed and trained with regard to fraud risk;
- Being aware of potential risks of fraud within their business unit;
- Enacting effective monitoring, review and control procedures to both prevent acts of fraud and detect acts of wrongdoing promptly should prevention efforts be unsuccessful;
- Ensuring learnings and feedback from suspected and confirmed fraud cases are appropriately rolled out within the business unit.

The authority to carry out the above responsibilities can be delegated to appropriate individuals within each Business Unit, however, the accountability for their effectiveness must remain with the Managing Director of the Business Unit.

Ultimately, it is the responsibility of every employee, consultant, agent and Director of the Group to immediately report any suspected fraud, misconduct or dishonesty, initially to their line manager or via the Group's whistleblowing hotline.

Monitoring of Fraud Risk

Fraud risk is a mandatory requirement for inclusion within all Business Unit Risk Registers. The identification and mitigation of potential fraud risks remains the responsibility of the Business Unit Managing Directors.

Risk Registers, including the identified Fraud Risks, will be reported to the Audit & Risk Committee regularly.

Reporting incidents of Fraud or Wrongdoing

In cases of fraud, it is often information gathered within the first 48 hours which provide the most useful data to bring about a satisfactory conclusion, as this is often before the perpetrator has had time to react to the allegations.

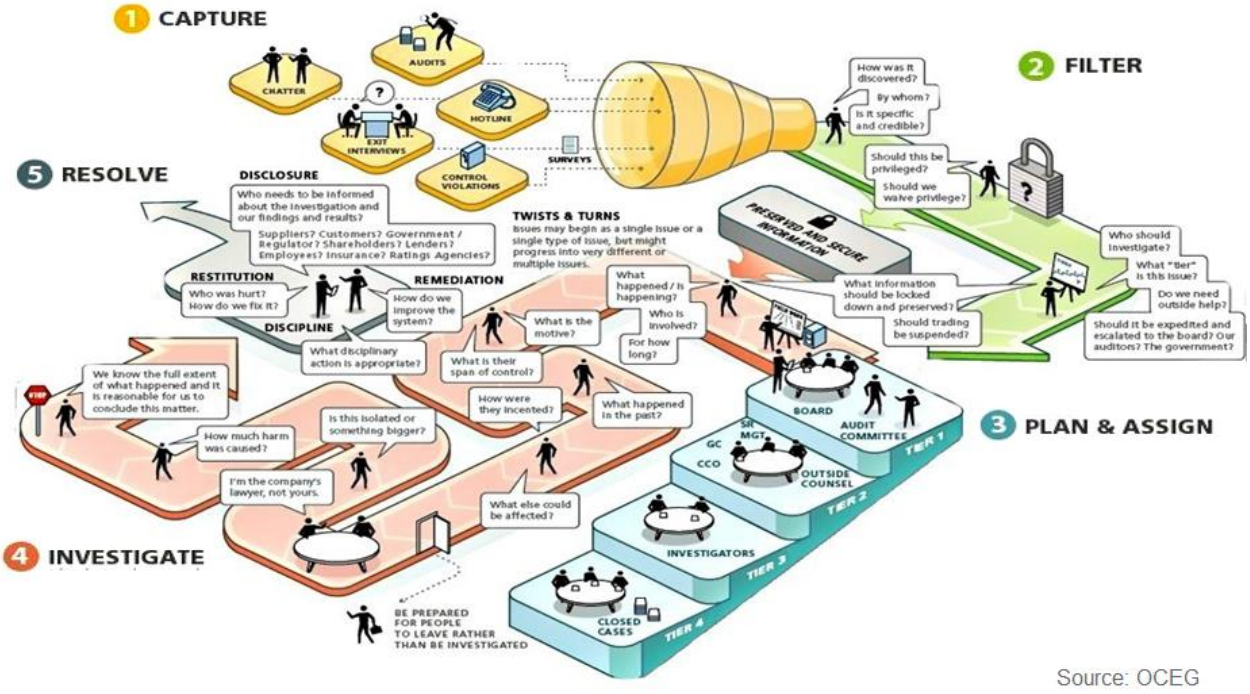
It is the responsibility of every employee within the Group to immediately report any suspected fraud or misconduct to their line manager or via the Group's whistleblowing hotline. Managers upon being made aware of such potential acts must immediately report to the Group Legal Counsel. Due to the important and yet sensitive nature of such suspected violations, it is essential we maintain a logical and professional approach to investigations. Employees, Managers and Directors must not

perform their own investigation work outside of the process set out within this document, as that can be one of the biggest threats to correct and proper incident handling.

Conducting Investigations

To ensure that all reported instances are treated equally and in a professional and independent manner the Group has agreed an investigation process which follows best practice guidelines from the OCEG (Open Compliance and Ethics Group).

The OCEG framework consists of 5 key areas to successful fraud investigation:



Source: OCEG

Investigation Stages

Stage 1: Capturing information

Information relating to potentially fraudulent activities can be collected from a number of sources across the Group including:

- Reports to the whistleblowing hotline;
- Concerns raised to operational management;
- Information collected from exit interviews;
- Findings from internal and external audits;
- Control violations identified by management in day-to-day activities.

It is important that while we're capturing information relating to potential frauds that we make a conscious effort to avoid pitfalls such as:

- Not focusing on the full range of data sources, making sure that we don't miss a serious issue;

- Missing the 'big ones', making sure that we have the right (competent and independent) people in place to review and filter information as its received;
- Making everything a big issue;
- Assigning the wrong people to investigations, some investigations will require technical knowledge;
- Allowing management override of controls to interfere with the investigation or its objectivity;
- Carrying out a superficial investigation without getting to the root cause of the issue; and
- Destroying the chain of evidence.

At this stage all information reports received should be treated as confidential and forwarded to the Group Legal Counsel, who will facilitate the initial triage process.

Stage 2: Filtering the information

Once a report has been received it is important that it is understood and filtered by a competent and independent source before the investigation begins. To help maintain a consistent approach the Group Legal Counsel (supported by additional independent individuals if required) will conduct a filtering exercise on all information received which will include:

- Ascertaining how the issue was discovered, and if it is specific and credible;
- Identifying who should be involved in the investigation (from an internal and external perspective); and
- Who needs to be made aware of the incident at this stage (e.g. the Board, external auditors, regulators etc).

After the initial investigation the Group Legal Counsel will make a decision in relation to further investigation of the reported issue.

Stage 3: Plan and Assign

Before any formal investigation can begin, an investigation plan (including planned communications), roles and responsibilities must be agreed. Roles and responsibilities should cover the investigation itself and the processing of any remedial issues identified during the investigation (even if the specific members of the operational team are not involved in the investigation itself).

Stage 4: Investigate

Key considerations for the first 48 hours

The first 48 hours of any investigation are critical, yet this is when many mistakes are made. During the first 48 hours it is crucial that we:

1. Fully understand the allegation
2. Identify the protocols, milestones and skills, and
3. Build the right team to fully investigate the issue.

Fully Understand the allegation

To enable a productive investigation, we need to first ensure that:

- The nature of the investigation is fully understood;
- Who may be involved in the incident, and what (if any) immediate operational changes need to be implemented;
- Which businesses of the Group may be affected;

- What data may be relevant, and how can it be secured;
- Potential commercial (or other) impact; and
- Who needs to be made aware of the allegation.

Identify the Protocols, Milestones and Skills

As part of the initial consideration of the investigation protocols, milestones, and skills needed to effectively investigate the incident must be established. For example:

Protocols	• Privilege • Retention policies • Data privacy • Escalation
Milestones	• Initial observations within 2 weeks • Agree frequency of further updates, and the most appropriate audience.
Skills	• Investigative interviewing skills • Forensic review and analysis • Financial modelling • Asset tracing • Business intelligence and background checks • Dispute readiness and advice • Forensic data technology • Experience in operational specialisms • Experience of subjects such as fraud, bribery and corruption, and counterfeiting.

Build the right team

The right investigation team will vary depending on the complexity of the incident being investigated. As with stages 2 and 3 the Group Legal Counsel will be responsible for coordinating stages 3 and 4.

Roles and Responsibilities

Specific roles and responsibilities will vary from investigation to investigation. However, they will reflect the roles and responsibilities detailed in the main body of this policy and will be formally agreed during the plan and assign stage of the investigation.

Stage 5: Resolve

As a result of each investigation a formal output will be produced, which at a minimum will detail the allegations, the findings of the investigation, and an outline of any identified issue which needs to be resolved by operational management.

Whistleblowing

Full details of the Group's Whistleblowing policy can be found on SharePoint, but for reference the Whistleblowing hotline can be reached on 0800 915 1571.

Confidentiality

The Group treats all information received with the utmost confidentiality. Any reprisal against any employee or other individual reporting an incident in good faith is strictly forbidden.

The identity of the employee who has brought the allegation will remain confidential. Investigation results will not be disclosed or discussed within anyone other than those who have a legitimate need to know within the bounds of the investigation. This is essential in order to avoid damaging the reputations of persons suspected, but ultimately found innocent and to protect the Group from potential civil liabilities.

Disciplinary action

If a fraud investigation results in the recommendation to dismiss or otherwise discipline an employee, the recommendation will be reviewed for approval by the appropriate representative from Human Resources and the Group Legal Counsel before such action is taken.

The Business Unit does not have authority to dismiss an employee for fraudulent activity without prior approval from the Group Legal Counsel.

Approved by the Board of Hargreaves Services plc

…….
R McDowell

Chair
27 March 2024