IMC GROUP

Fraud Risk Management Policy

Version Control Log

Version No.	Updated by	Signature	Approved by	Signature	Date of Last Edit
01/2020	Oon Chen Yen Head Group Risk Management Tay Teng Hwee Group Risk Manager		Loh Niap Juan Group Chief Corporate Officer		1 December 2020

Key Distribution List

All staff members of IMC Group are authorized to have a copy of this document.

Document Owner:

IMC Group Risk Management

Contents

1. Purpose of Policy, Policy Statement & Objectives

1.1 Background to Policy

(a) With ever increasing complexity and changes in the environment, fraud is recognised as posing a significant threat to organisations. Fraud is part of operational risk and must be managed.

(b) Fraud prevention, detection and management is the responsibility of all employees in all IMC Business Units and Functional Departments. Staff who are informed and aware provide the best protection against fraud and corruption. In addition, the senior management of the IMC Group has the ultimate responsibility for maintaining the security and integrity of the IMC Group's business processes and to ensure that assets of the IMC Group are safeguarded by adopting and implementing appropriate controls and review procedures.

(c) As there is no universal definition as to what constitutes fraud, it is important that IMC defines fraud from its own ethical perspective so that all employees have a common understanding of fraud and adopt a consistent approach towards preventing and mitigating the risk.

1.2 Purpose of Policy

The purpose of this Policy is to underline the need for all employees to:

(a) Display the highest standard of personal and corporate integrity/ethics;

(b) Comply with all laws and regulations and internal controls, policies and procedures;

(c) Be open and honest in all internal and external dealings thus developing collectively a culture of risk awareness, openness, transparency and trust.

1.3 Policy Statement

(a) Where fraud is concerned, IMC adopts a **"zero-tolerance"** stance.

(b) It must be emphasized that fraud is totally unacceptable, and all instances of suspected fraud will be treated seriously and dealt with swiftly. IMC will investigate all allegations of fraud and where fraud is evident, IMC's policy is to take firm action against the person(s) involved. This includes referring the matter to the appropriate law enforcement and/or regulatory agencies for investigation and prosecution.

(c) In addition to disciplinary actions meted out to employees who engage in fraudulent misconduct, managers of the relevant Business Unit or Functional Department may, in certain circumstances, be held accountable for failing to ensure that the applicable controls have been complied with.

1.4 Policy Objectives

The objectives of this Policy are as follows:

(a) To establish a common understanding of fraud in order to:

- Identify and assess potential sources of fraud;
- Communicate clearly that fraud is unacceptable and the serious consequences for would be perpetrators;
- Achieve a consistent approach towards managing the risk of fraud.

(b) To establish the key components of fraud risk management;

(c) To establish the fraud risk prevention and mitigation principles and design effective mitigating controls to reduce the opportunities to commit fraud and detect its occurrence;

(d) To establish reporting, investigation and disciplinary procedures for fraud and suspected fraud incidents.

2. Related Policies

2.1 This Policy should be read in conjunction with the following:

- IMC Group Code of Business Conduct
- IMC Group Whistle Blowing Policy

2.2 The IMC Group Code of Business Conduct sets out the values and ethical standards which all IMC personnel are expected to commit to and maintain.

2.3 The IMC Group Whistle Blowing Policy provides employees with a confidential channel for raising concerns relating to suspected irregularities, misconduct or fraud, without the fear of reprisal or intimidation.

3. What Constitutes Fraud

3.1 Definition of Fraud

(a) For the purpose of this Policy:

Fraud means:

(i) **any act of misconduct or dishonesty**, or

(ii) **any act of deliberate misrepresentation, falsification, concealment or destruction of information and/or documentation,**

which is carried out in order to **cheat, deceive or mislead any party** with the aim of obtaining assets, property (including intellectual property), money or other gains or benefits from that party or any other party.

(b) Acts of fraud can be perpetrated by:

- Employees and crew;
- Customers, suppliers or other third parties;
- Collusion between any of the above parties, internally or externally.

3.2 Fraud Categories

(a) Broadly, fraud is categorized as follows:

- Internal Fraud
- External Fraud

(b) The definitions and examples (non-exhaustive) of the above are provided in the following table:

Broad Fraud Categories	Definition	Sub-Categories	Examples (non-exhaustive)
Internal Fraud	Acts of a type intended to defraud, misappropriate property or circumvent any	Un-authorised Activities	• Transactions not reported intentionally • Transaction type being unauthorised that results in or could lead to monetary loss by the company • Hacking/spreading viruses into company's IT systems

Broad Fraud Categories	Definition	Sub-Categories	Examples (non-exhaustive)
	laws, regulations, or policies (including corporate policies), which involves at least one internal party (whether acting in collusion with an external party or not)		• Unauthorised deletion/destruction of company files (physical or soft copies) • Intentional breach of internal system security • Deferment of business profits/losses to meet current targets • Manipulation of business profits to enhance performance bonuses to which they are otherwise not entitled • Manipulation of company records or reconciliations to conceal losses or improve profits • Unauthorised diversion of company funds • Unauthorised alteration of documents • Falsification of documents • Conclusion of contracts or transactions at off-market rates without prior approval • Deliberate mispricing in quotations and proposals to external parties • Unauthorised use of other company's name/logo in business dealings • Activity with unauthorised counterparty • Intentionally misleading the management, colleagues or the auditors • Inappropriate or favourable treatment of associated parties for personal benefit • Unauthorised or inappropriate access to or release of information
		*Theft and Fraud	• Theft/extortion/embezzlement/ robbery/smuggling involving company's property including intellectual property rights for software • Unauthorised transfer or sale of company assets • Presentation of original documents, cheques and other valuables for unauthorised transactions (e.g. due to theft or embezzlement)

Broad Fraud Categories	Definition	Sub-Categories	Examples (non-exhaustive)
			• Misappropriation of company's funds and assets • Falsification of expense and expenditure items • Deliberate tax non-compliance/evasion • Payroll fraud • Payment fraud via cheque or electronic payment mode • Software programming fraud • Forgery of any kind including signature, document and transaction • Act of sabotage • Account take-over/impersonation of account holder • Bribes/Kickbacks* (corruption) • Transactions benefiting the perpetrator at expense of company (e.g. an employee has an undisclosed financial interest in a transaction or arrangement that causes harm to the business, often because the price is not the best the company can get) ** This includes what is prohibited under the prevailing anti-corruption legislation in the respective jurisdictions in which IMC operates (e.g. Singapore Prevention of Corruption Act and US FCPA)*
External Fraud	Acts of a type intended to defraud, misappropriate property or circumvent any laws, regulations, or policies (including corporate policies), which	Theft and Fraud	• Theft of company's property including intellectual property rights • Payment fraud via cheque or electronic payment mode • Forgery of any kind including signature, document and transaction • Includes examples listed under Internal Fraud
		Systems Security	• Hacking/Introducing virus into company's systems • Theft of company information

Broad Fraud Categories	Definition	Sub-Categories	Examples (non-exhaustive)
	are committed by a third party.		• Security breach (whether by an internal or external party) • Phishing

(c) Vigilance is therefore required against both Internal Fraud and External Fraud. The roles and responsibilities of the respective stakeholders in managing fraud risk are set out in Section 4 of this Policy. Further, a Fraud Risk Management Framework is set out in Section 5 of this Policy as a framework for IMC Business Units and Functional Departments to adhere to.

4. Roles and Responsibilities

The primary roles and responsibilities of the various stakeholders within IMC in relation to the management of fraud risk are as follows:

4.1 All Employees

(a) First level defence against fraud and misconduct.

(b) Understand the relevant business processes and comply with all required internal controls, policies and procedures.

(c) Be familiar and understand IMC's fraud reporting and whistle blowing process, as set out in this Policy and in the IMC Group Whistleblowing Policy.

(d) Escalate any observation of suspected irregularities, misconduct or fraud to immediate superiors and/or Business Unit/Functional Department Heads, or alternatively, submit a report through the Whistleblowing channel in accordance with the IMC Group Whistle Blowing Policy.

(e) Cooperate fully with all investigations.

4.2 Management of Business Units and Functional Departments

(a) Comprises Business Unit/Functional Department Heads and management.

(b) Promote a culture of Ethics and Compliance within their respective Business Units/Functional Departments.

(c) Create an environment where employees feel comfortable raising concerns and have opportunities to discuss issues relating to Ethics and Compliance.

(d) Own, develop and maintain internal controls, policies and processes, and ensure that they remain relevant through periodic self-assessments.

(e) Ensure compliance with all internal controls, policies and procedures.

(f) Be alert for deviant behaviours and ensure that such behaviours are not tolerated and that employees are counselled and/or disciplined early to mitigate possible risks.

(g) Perform initial assessment of any suspected irregularities, misconduct or fraud that have been reported to them and take the necessary steps to deal with such reports, including initiating reports in accordance with the IMC Group Whistle Blowing Policy and supporting investigations into suspected irregularities or misconduct. Where necessary, escalate the matter to senior management for further direction.

(h) Assess the results of investigations into suspected irregularities, misconduct or fraud and, in consultation with senior management, determine the remedial actions to be taken, as well as the disciplinary actions to be taken against the personnel in question, if any.

(i) Implement remedial and disciplinary actions promptly.

4.3 Senior Management

(a) Comprises Corporate Office/SBG/SBU Heads and management.

(b) Promote a culture of Ethics and Compliance throughout IMC.

(c) Oversee and monitor compliance by Business Units and Functional Departments with all internal controls, policies and procedures.

(d) Assess any matter escalated to them by Business Unit/Functional Department management, or in accordance with the IMC Whistleblowing Policy, and provide such direction and support as may be required.

(e) Support and ensure that resources are allocated for investigations into incidents of suspected irregularities, misconduct or fraud, as and when required.

(f) Assess the results of investigations into suspected irregularities, misconduct or fraud and direct and support Business Unit/Functional Department management in determining the remedial actions to be taken to and the disciplinary actions to be taken against the personnel in question, if any.

(g) Ensure that remedial and disciplinary actions are implemented promptly by Business Units and Functional Departments, as well as relevant internal stakeholders (e.g. People & Development) and that the “lessons learnt” are shared to all employees.

4.4 Group Risk Management

(a) Second line of defence against fraud and misconduct (primarily through the Enterprise Risk Management framework).

(b) Provide on-going fraud advisory support to Business Units and Functional Departments.

(c) Assist in the fraud reporting and investigation process as may be required.

(d) Promote fraud awareness and understanding through fraud education and awareness.

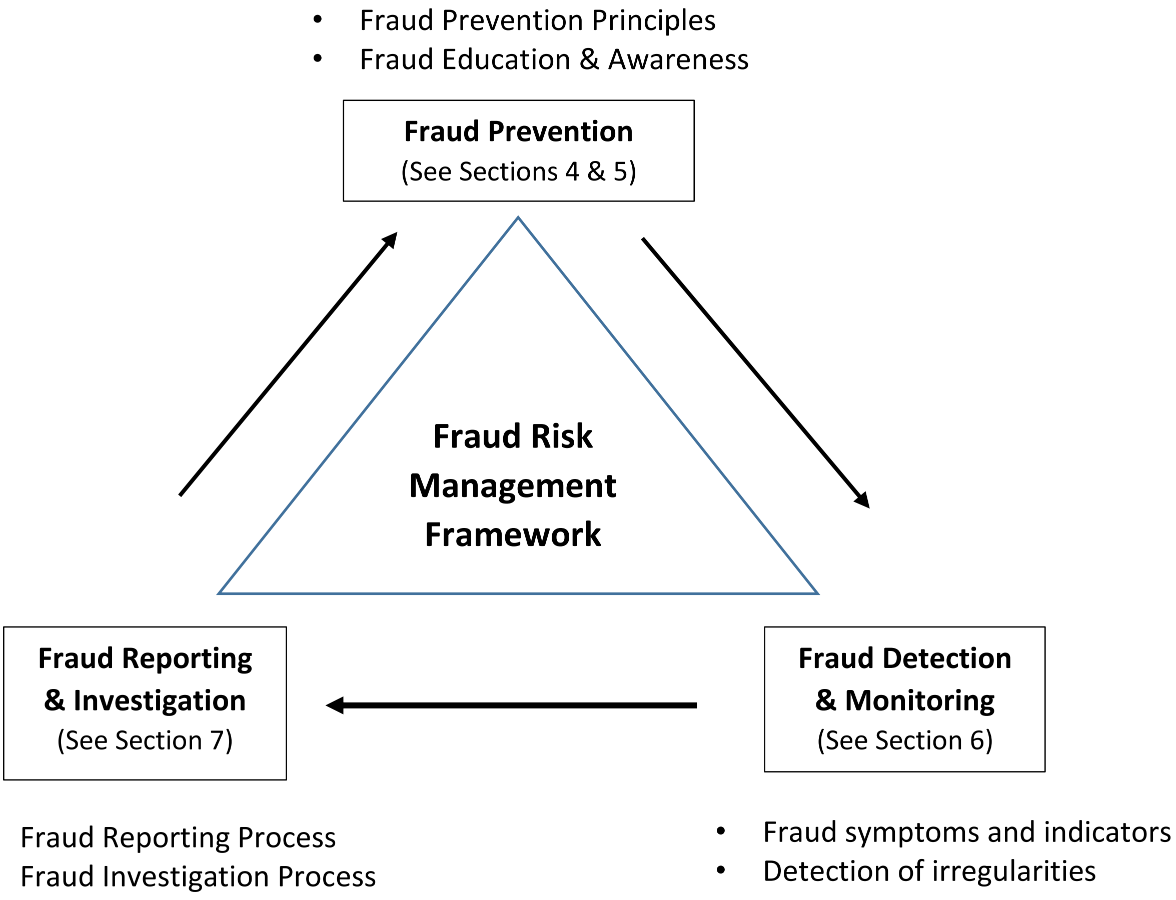
4.5 Group Internal Audit

(a) Third line of defence against fraud and misconduct (primarily through the internal audit process).

(b) Assist in the fraud reporting and investigation process in accordance with the IMC Whistleblowing Policy and as may otherwise be required.

5. Fraud Risk Management

5.1 Fraud Risk Management Framework



- Fraud Prevention Principles
- Fraud Education & Awareness

Fraud Prevention
(See Sections 4 & 5)

Fraud Risk Management Framework

Fraud Detection & Monitoring
(See Section 6)

- Fraud symptoms and indicators
- Detection of irregularities

Fraud Reporting & Investigation
(See Section 7)

- Fraud Reporting Process
- Fraud Investigation Process

(a) The IMC Fraud Risk Management Framework comprises of 3 major components:

1. **Fraud Prevention** – embed control mechanisms and principles to seek feasible ways to deter fraudulent acts and to mitigate possible impact on the organisation

2. **Fraud Detection & Monitoring** – implement detection techniques to uncover fraud events when preventive measures are not available or not working

3. **Fraud Reporting & Investigation** – uphold reporting process and support recovery actions, which may include insurance claims, civil suits, seizures of assets through criminal case action or collection activities, performed by the appropriate parties

(b) As the responsibility of preventing, detecting, monitoring and responding to fraud resides with all IMC Business Units and Functional Departments, the above components must be embedded in their Business-As-Usual (BAU) processes. Fraud risk should be incorporated into the Enterprise Risk Management (ERM) framework, with the salient controls being identified and implemented. Such controls should be capable of being tested and verified in the course of the ERM programme as well as internal audit reviews.

5.2 Fraud Prevention Principles

In order to ensure that fraud opportunities do not arise, the following prevention principles should be strictly observed by all IMC Business Units and Functional Departments and incorporated into their business processes and internal controls.

5.2.1 Work control principles

(a) **Dual Control**

The dual control principle must be applied in all important business transactions, i.e. after due processing by an employee, a business transaction must be checked and countersigned/released by at least another authorised employee. Both employees are jointly responsible for all aspects of the business transaction.

(b) **Functional Segregation**

- Functional segregation is the allocation of activities to different areas of responsibility.

- Functions must be segregated in scenarios where:

  - Regulatory requirements must be fulfilled;

  - Conflicts of interest must be avoided.

(c) **Control Principles**

- Controls must always be carried out in full. Controls must not be curtailed, circumvented, or partially executed on the strength of long term personal relationships or instructions (which are in breach of regulations) from superiors. Routine checks and monitoring to ensure that procedures are being followed are essential.

- Serious breaches of the company's internal control standards must be notified to the direct superior or depending on the circumstances, to the latter's direct superior who must take all necessary action to assess and address the risk. Where necessary, the report is to be escalated to senior management for further action. Alternatively, employees may submit a report through the Whistleblowing channel in accordance with the IMC Group Whistle Blowing Policy. See Section 7 for further details.

5.2.2 Management of business processes – Know your process

(a) Understanding the relevant business processes, identifying and implementing the key controls necessary to combat the various types of fraud is essential. Each IMC Business Unit and Functional Department needs to ensure that the business processes meet with the applicable control standards. Reviewing the business processes from "cradle" to "grave" enables us to assess the risk of fraud and identifying the appropriate controls.

(b) A cross-functional view of risk is to be adopted in order to break down organisational and functional barriers and better manage the risk of fraud. Functional hierarchies and operational silos can be a breeding ground for unmanaged risks, including the risk of fraud. The enterprise nature of risk and effective management of risks therefore require a business process rather than a functional or departmental view. Accordingly, Business Units and Functional Departments should take a business process perspective that cuts across functional or departmental boundaries.

5.2.3 Business transaction processing

(a) It must be ensured that only authentic orders/vouchers (whether from customers, suppliers or others) are accepted for processing.

(b) Orders/vouchers may only be processed when the signing requirements have been fulfilled. Processing units must be informed who is authorised to sign and must refer to the appropriate Authority Matrix where required for certainty.

(c) It is also important to engage customers and suppliers in the control process. Processes for the review and verification of statements/advices together with clarifications and confirmations from customers and suppliers, as well as robust payment mechanisms, should be established.

5.2.4 Unusual transactions – Know your customer

(a) Transactions which deviate substantially from the normal business relationship with a customer or supplier must be reviewed with more than just the normal level of control. Additional authentication checks must be put in place.

(b) Special care is required if substantial amounts are received for unknown customers or for customers with unknown creditworthiness and are to be withdrawn or transferred by the latter, especially in connection with newly opened accounts. Unusual inquiries, (e.g. dubious offers from third parties) should only be answered after consultation with management and checking with the customer or supplier, if necessary.

5.2.5 Storage of valuable assets

(a) All valuable assets and important business documents must always be stored responsibly and in such a way that unauthorised persons cannot gain unimpeded access.

(b) Safes and strong boxes must always be protected by a double lock arrangement. Each holder of the locking media must participate personally in the locking and unlocking process.

(c) The following types of items, documents and assets should always be stored securely:

- Legal documents e.g. share certificates, corporate secretarial records, land titles, lease agreements, charter parties, commercial contracts and agreements etc.;
- Company seals and company stamps;
- Accounting and financial records;
- Employee personal data and records;
- Media and documents to which individuals are not allowed to have access for reasons of internal operating security *(e.g. reserve keys, PIN letters, Root & master passwords)*.

5.2.6 Access controls

(a) Implementing effective access controls is essential in ensuring that only authorised employees have access to IMC’s critical assets.

(b) Such physical and logical access controls should cover access to office premises, computer systems and databases, and the company Intranet at the minimum.

(c) As the use of information technology is prevalent and ever changing, particular emphasis has to be placed on information/system security and integrity which should encompass the rigorous utilisation of user profiles, passwords, firewalls and other measures to prevent unauthorised access.

5.2.7 Signatory powers/ Authorisation limits

(a) Granting of signatory powers and limits of authority must be appropriate and based on the employee's level of experience, expertise and functional responsibility. As these rights confer powers of representation, it is essential that the authorised signature list and limits of authority be kept updated and current.

(b) Further, a double-signature or dual-authorization process should be set as the key control point to govern all withdrawals and payments.

(c) In addition, for execution of material transactions, contracts or agreements, the employees responsible for the execution should check whether they have been duly authorised (whether under the applicable authority limits or a Power of Attorney or otherwise) to execute such transaction, contract or agreement.

5.2.8 Pre-employment screening

Appropriate pre-employment reviews and screening should be carried out with emphasis on recruiting employees with integrity. References should be checked and the plausibility of the reason for change validated particularly if the move would entail a substantial drop in remuneration. Subsidiaries where local regulations mandate more stringent checks are to comply accordingly.

5.2.9 Know your employee

Internal fraud often succeeds because of inadequate supervision that fails to identify performance and/or behavioural issues that might indicate/lead to potential wrongdoing. In this regard, particular emphasis has to be placed on the employee appraisal and monitoring process which provides an opportunity for employee to voice their grievances and culminating in a common understanding and resolution of their concerns.

5.2.10 Intimidation & Inducements

(a) Senior Management must ensure that personnel occupying key control and reporting functions, have not only the technical skills to perform their function, but also possess a strong sense of integrity, professionalism and personality to resist intimidation and inducements to act in a manner that would subvert the internal control structure. This may be particularly difficult if the intimidation or inducement emanates from a more senior employee.

(b) Personnel placed in such a position should report this to their immediate superior or, depending on the circumstances, to a sufficiently higher level of management to ensure that all necessary steps are taken to curb this practice. Alternatively, reports may be made through the Whistleblowing channel in accordance with the IMC Group Whistle Blowing Policy (see Section 7 for further details).

5.2.11 Code of Business Conduct

The erosion of ethical behaviour will result in progressive misconduct that may lead to employees committing fraud. To further inculcate sound conduct and ethical practice, the IMC Code of Business Conduct must be put into practice. Employees should refer to and familiarise themselves with the values and ethical standards set out under the IMC Code of Business Conduct.

6. Fraud Detection

While all employees are expected to be aware of the potential for fraud and to take the necessary steps to report any suspected fraud, the primary responsibility for detecting fraud lies with management through the implementation of effective systems of internal control. Group Risk Management being the second line of defence and Group Internal Audit being the third line of defence will also assist in preventing and detecting fraud through their review and evaluation of the internal control framework.

6.1 Fraud Detection Procedures

Management should ensure that appropriate fraud detection procedures are incorporated within their Business-As-Usual (BAU) processes. The following approach may be undertaken in developing such procedures:

(a) Firstly, the key areas of exposure to fraud should be identified.

(b) Secondly, recognizing the symptoms of fraud and what fraud may look like, for example: lack of segregation of duties, lack of physical safeguards, lack of independent checks, lack of proper authorization, lack of proper documents and records, and overriding of existing controls.

(c) Thirdly, build detective processes to look out for symptoms and behaviours that are indicative of potential fraud, and be alert for these.

(d) Fourthly, once symptoms or behaviours that are indicative of fraud are observed, there must be appropriate follow-through in order to ascertain whether or not there is actual fraud, either by way of further investigation or other means.

6.2 Warning signs of potential fraud

Potential warning signs of fraud include but are not limited to:

(a) An employee whose lifestyle is at variance with their known source of income;

(b) Changes in lifestyle or habits of employee (e.g. gambling, stock market trading);

(c) Excessive or unusual hours worked by employee and/or a lack of delegation of apparently mundane tasks; Inadequate segregation of duties;

(d) Suspicious documents or signatures that do not match the person's usual signature;

(e) Secrecy about a particular client/project or whether the client will only deal with a particular employee;

(f) Inadequate documentation about a client or transaction;

(g) Instances of internal controls that have been overridden by management;

(h) Key reconciliations are not completed in a timely manner;

(i) Unusual transactions with parties that are related to an employee, e.g. family members, companies controlled by such employee or family members;

(j) Payments for services that appear excessive in relation to the services actually provided;

(k) No enforcement of mandatory leave (where applicable) and alternative cover procedures during absences, and work is left until the employee returns;

(l) Unusual transactions that have a significant effect on earnings;

(m) Unusually high or unexpected levels of profits or losses;

(n) Profits and cashflow at variance with each other.

7. Fraud Reporting Procedure and Investigation Process

7.1 Procedure for Fraud Reporting by Employees and Investigation Process

7.1.1 Reporting Channels

It is the obligation of ALL employees to report any suspicion of fraud, misconduct or irregularities. An employee may either choose to report a fraud or misconduct incident (or suspected incident) anonymously or directly.

7.1.2 Anonymous Reporting by Employees

If the employee wishes to remain anonymous, he or she may submit a report of a fraud or misconduct incident (or suspected incident) through either of the following channels:

(a) Through submitting a report to Lighthouse (formerly known as InTouch) (or such other service provider as may be appointed from time to time) via the channels set out in the IMC Group Whistle Blowing Policy, in which case IMC will be required to deal with such reports in a way that will protect the identity of the employee *(whistleblower)* and provide for the security and confidentiality of the information provided.

(b) Reporting to Group Internal Audit (Group IA), in which case Group IA will proceed to file the report with the Lighthouse (formerly known as In-Touch) platform and thereafter the matter will be dealt with in accordance with the IMC Group Whistle Blowing Policy.

UPDATE: InTouch has been renamed as Lighthouse and the following channels are available for submission of reports:

Website: www.lighthouse-services.com/thecode
Email: reports@lighthouse-services.com

7.1.3 Direct Reporting by Employees

(a) An employee may choose to report of a fraud or misconduct incident (or suspected incident) to his or her immediate supervisor. Upon a report being received by a supervisor, the supervisor shall escalate the report to the relevant Business Group / Business Unit / Corporate Function Head for further action. The relevant Head shall forward the report to the Head, Group Corporate Office, copying both Head, Group Internal Audit and Head, Group Risk Management (collectively, "**Group Corporate Office**").

(b) The relevant Head shall consult with Group Corporate Office whether the report warrants further investigation. If further investigation is warranted, this will be carried out in accordance with Section 7.2 below.

7.1.4 Direct Reporting by Business Units / Corporate Functions

(a) Actual or suspected fraud, misconduct or irregularities may affect a Business Unit or a Corporate Function directly. For example, a third party may impersonate a business counterparty and either fraudulently induce, or attempt to fraudulently induce, the Business Unit or Corporate Function to make payments to that third party instead of the business counterparty. In such event, the relevant employees MUST escalate the incident directly to the Head of the Business Group / Business Unit / Corporate Function.

(b) Upon the receipt of the report, the relevant Business Group / Business Unit / Corporate Function Head shall forward the report to the Head, Group Corporate Office, copying both Head, Group Internal Audit and Head, Group Risk Management.

(c) The relevant Head shall consult with Group Corporate Office whether the report warrants further investigation. If further investigation is warranted, this will be carried out in accordance with Section 7.2 below.

(c) The relevant Head shall consult with Group Corporate Office whether the report warrants further investigation. If further investigation is warranted, this will be carried out in accordance with Section 7.2 below.

7.2 Investigation Process

The investigation process of each report of suspected fraud, misconduct or irregularities filed with the Lighthouse platform under Section 7.1.2 shall be carried out in accordance with the IMC Group Whistle Blowing Policy. This investigation process set out in this Section 7.2 shall apply to direct reports filed under Sections 7.1.3 and 7.1.4.

7.2.1 Investigation Committee

(a) If, after consultation between the relevant Head and Group Corporate Office, it is determined that the report warrants further investigation, an Investigation Committee will be constituted to investigate the matter.

(b) Members of the Investigation Committee shall comprise representatives of both the Business Unit / Corporate Function in question and Group Corporate Office.

(c) In carrying out its investigation, the Investigation Committee has the authority to seek any relevant information it requires from any employees and all employees will be directed to cooperate with any request made by the Investigation Committee.

(d) The status of the investigation conducted pursuant to a report filed above or the results thereof will not be provided to anyone other than those who have a legitimate need to know.

7.3 Actions from Fraud Investigation

7.3.1 Following its investigation of the matter at hand, the Investigation Committee will recommend the actions, if any, that should be taken, both relating directly to the matter being investigated and more generally, to prevent and detect similar incidents.

7.3.2 Group Corporate Office and the relevant Business Group / Business Unit / Corporate Function Head(s) shall consider the Investigation Committee's recommendations and determine the final decisions to be taken by IMC on the matter at hand. These may include the below:

(a) **Feeding back to the person raising the initial concern**

How and what stage to provide, in confidence, feedback to the person(s) who raised the initial concerns.

(b) **Disciplinary action**

- Fraud is considered gross misconduct and it is IMC's policy to take firm action as a deterrent against future incidents of fraud.
- Accordingly, fraudulent misconduct on the part of an employee will lead to disciplinary action or summary dismissal. The relevant Business Group, Business Unit or Corporate Function Head will oversee the process, working with People & Organisation and the individual's line manager. Where necessary, guidance is to be sought from Group Corporate Office.
- Where deemed necessary, the investigation results shall be referred to the appropriate law enforcement and/or regulatory agencies for independent investigation and prosecution. This will be especially the case where IMC may be exposed to potential liability by such fraud and/or the reputation of IMC may be tainted by such fraud. In such cases, legal advice will be sought to protect the rights of IMC and to ensure that any criminal investigation or prosecution (whether potential or ongoing) will not be compromised.

(c) **Civil recovery**

Recovering losses is a major objective of any fraud investigation. Where the loss is substantial, legal advice will be obtained about the need to freeze, and feasibility of freezing, through the courts, the subject's assets, pending conclusion of the investigation. Legal advice will also be obtained about the prospects of recovering losses through the civil court, where the subject refuses repayment. IMC will seek to recover its costs in addition to any losses as a result of the fraud. Insurers should also be notified as soon as possible (where relevant).

(d) **Strengthening the system and learning lessons**

Where the investigation identifies vulnerabilities in a particular system or process, or a lack of safeguards, at the direction of Group Corporate Office, the relevant Business Group, Business Unit or Corporate Function Head will draw up an action plan to address the vulnerabilities. He or she will report back to senior management on progress in implementing the actions. He or she will also ensure any wider lessons are learned and acted on.