ANTI-FRAUD POLICY AND PROGRAM

This policy is established to facilitate the development of controls that will aid in the prevention and detection of fraud against the Company.

Contents

ANTI-FRAUD POLICY

I. Overview

The National Reinsurance Corporation of the Philippines (the "Company") endeavors to promote the culture of good corporate governance by upholding the highest principles of accountability, integrity, and honesty, and complying with laws and regulations to serve the best interests of its stakeholders. In accordance with these values and laws, the company's Anti-Fraud Policy (the "Policy") is established to facilitate the development of controls that will aid in the prevention and detection of fraud against the Company. It is the intent of the Company to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigation.

The Insurance Commission prescribes the minimum standards to be adopted by companies in developing guidelines for preventing (insurance) fraud or fighting it in case it occurs. *(IC Circular Letter No. 2016-50 on Guidelines in the Development of Anti-Fraud Plan for Insurance Companies)*

II. Scope

This policy applies to any irregularity, or suspected irregularity, involving customers (insurers/reinsurers or intermediaries), employees, directors, shareholders, consultants, vendors, contractors, outside agencies and/or other parties with a business relationship with the Company.

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

III. Definition of Terms

FRAUD- is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain. (*definition by the Association of Certified Fraud Examiners –ACFE)*

There are three broad categories of fraud as described under the related IC Circular and these are:

a. **Policy holder and claims fraud**: fraud against insurer by policyholder and/or other parties in the purchase and/or execution of an insurance product, including fraud at the time of making a claim;
b. **Intermediary fraud**: fraud perpetrated by intermediaries against insurer/reinsurer and/or policyholders;

c. **Internal fraud:** fraud/misappropriation against insurer/reinsurer (employer) by an employee, manager or officer on his/her own volition or in collusion with parties that are internal or external to the insurer/reinsurer. This is also called ***occupational fraud.***

OCCUPATIONAL FRAUD- is further defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.

The three major types of occupational fraud, frequently referred to as the **Fraud Tree** (*an occupational fraud and abuse classification system developed by the Association of Certified Fraud Examiners- ACFE)* are the following:

a. **Corruption**- includes conflict of interest, bribery, illegal gratuities and economic extortion
b. **Asset Misappropriation**- includes Cash, Inventory and all other assets
c. **Financial Statements Fraud**- includes overstatement or understatement of Net Worth/ Net Income

Some actions constituting fraud refer to, but are not limited to the following:

- Any dishonest or fraudulent act
- Misappropriation of funds, securities, supplies or other assets
- Impropriety in the handling or reporting of money or financial transactions
- Profiteering as a result of insider knowledge of company activities
- Disclosing confidential information and proprietary information to outside parties
- Disclosing to other person securities activities engaged in or contemplated by the company
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the company
- Destruction, removal, or inappropriate use of records, furniture, fixtures and equipment; and/or
- Any similar or related irregularity

IV. Policy Guidelines

Management is responsible for the prevention and detection of fraud, misappropriations and other irregularities. Each member of the management team should be familiar with the types of improprieties that might occur within his or her area of responsibility, and be alert for any indication of irregularity.

The Company takes a "no fraud tolerance" attitude. All suspicious or fraudulent activities, regardless of the aggregate monetary amount involved, should be reported and will undergo preliminary evaluation.

Any irregularity that is detected or suspected must be reported immediately to the Compliance Office, who shall coordinate all investigations with the Heads of Internal Audit (IA) and Human Resources (HR) and other affected areas. Legal advisers may also be consulted as necessary.

Fraud Awareness. Management establishes a fraud awareness program and determines who should attend, frequency and length, cultural sensitivities, guidance on how to solve ethical dilemmas and delivery methods. Documentation to support fraud awareness should define and describe fraud and fraud risks. It should also provide examples of the types of fraud that could occur and identify the potential perpetrators of fraud.

Fraud Risk Assessment. A fraud risk assessment should be performed on a systematic and recurring basis, involved appropriate personnel, consider relevant scheme and scenarios to mitigating controls. The existence of a fraud risk assessment and the fact that management is articulating its existence may deter would-be perpetrators.

A. Prevention of Fraud

Prevention is the most pro-active fraud-fighting measure. The design and implementation of control activities must be a coordinated effort of management. Collectively, all function heads should be able to address identified risks, design and implement control activities and ensure that techniques are adequate to prevent the fraud from occurring in accordance with the organization's risk tolerance. A fraud prevention program's success depends on its continuous communication and reinforcement.

Among the many elements in fraud prevention are *HR Procedures, authorization limits and transaction level procedures.*

1. The **HR** function plays an important role in fraud prevention by implementing the following **procedures-**
    a. Performing background investigation on prospective employees
    b. Conduct Anti-fraud training for employees
    c. Evaluating performance and compensation programs
    d. Conducting Exit interviews

2. **Authority Limits**- establish authoritative approval levels across the organization as an entity-level control. On the other hand, individuals working within a specific function may be assigned only limited IT

access as a process-level control. These types of control, supported by the appropriate segregation of duties, assist in the first line of defense in the fraud prevention.

3. **Transaction-Level Procedures**- review of third party and related party transactions can help prevent fraud. Preventive measures are especially needed for related-party transactions that can be controlled by board members or by employees of authority with an interest in an outside entity with which the company may conduct business. Such individuals may mandate transactions that ultimately benefit them at the expense of the company.

***Conflict Disclosure*.** A process should be implemented for directors, employees and contractors to internally self-disclose potential or actual conflict of interest for management to implement appropriate course of action.

***Reporting Procedure and Whistleblower Protection*.** The Company will implement its Whistle Blower Policy to encourage directors, senior officers, and employees to report knowledge of fraud perpetrated against the Company, and to promote a culture of honesty and vigilance in the workplace. To encourage timely reporting, the company will communicate the protection accorded to the individual reporting the issue and this will be covered under the whistleblower protection.

Internal Audit. The Internal Audit function will continue to help detect fraud through its regular audit and report findings on fraudulent activity directly to the Audit Committee.

B. **Fraud Detection**

Detection techniques must be established to uncover fraud events when preventive measures fail or unmitigated risks are realized. Important detection methods include *anonymous reporting mechanism (whistleblower policy), process controls and proactive fraud detection procedures* specifically designed to identify fraudulent activity.

1. ***Whistleblower Policy***. Provision for anonymity of any individual who willingly comes forward to report a suspicion of fraud is key to encouraging such reporting and should be a component of the company's policy. The most effective whistleblower policy preserves the confidentiality of anybody reporting and provide assurance to them that they will not be retaliated against for reporting their suspicions of wrongdoing including the wrongdoing of their superiors. To preserve the integrity of the

whistleblower process, it must also provide a means of reporting suspected fraud that involves senior management, possibly reporting directly to the Audit Committee.

2. ***Process Controls***. These are specifically designed to detect fraudulent activity, as well as errors, include reconciliations, independent reviews, physical inspections/counts, analyses and audits. A lack of, or weakness in preventive controls increases the risk of fraud and places a greater burden on detective controls. The more the significant the fraud risk, the more sensitive to occurrence (e.g., use of thresholds, performance frequency, and population tested) the detective control should be. There should be a systematic identification of the types of fraud schemes that can be perpetrated against or within the organization to identify the process controls needed to reduce and control the risks.

3. ***Proactive Fraud Detection Procedures***. Technology tools enhance the ability of management at all levels to detect fraud. Data analysis, data mining and digital analysis tools can: *(a) identify hidden relationships among people, organizations, and events; (b) identify suspicious transactions; (c) assess the effectiveness of controls; (d) monitor fraud threats and vulnerabilities; (e) consider and analyze thousands or millions of transactions.*

   Internal/External Auditors may have developed tools, as part of their fraud detection efforts, that analyze journal entries to mitigate management override of the internal control system. These tools identify transactions subject to certain attributes that could indicate risk of management override, such as user identification, date of entry and unusual account pairings.

4. ***Continuous Monitoring of Fraud Detection Techniques.*** Management should develop ongoing monitoring and measurements to evaluate, remedy and continuously improve the organization's fraud detection techniques. If deficiencies are found, management should ensure that improvements and corrections are made as soon as possible. A follow-up plan should also be in place to verify that corrective or remedial actions have been taken.

C. Investigation and Corrective Action

A reporting process should be in place to solicit input on potential fraud and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and timely.

1. ***Fraud Investigation and Response Protocols***. Potential fraud may come to the company's attention in many ways, including tips from employees, customers, or vendors; internal audits; process control identification; external audits; or by accident.

    i. There should be a process for tracking or a case management system in which all allegations of fraud are logged.

    ii. Examine and evaluate the allegations received to determine whether it involves a potential violation of law, rules, or company policy.

    iii. Generally, any irregularity that is detected or suspected must be reported immediately to the Compliance Office. He convenes the Evaluation Team, with the participation of both Heads of Internal Audit and Human Resources. The **Evaluation Team** recommends to the Board through the Audit Committee the final composition of the **Investigation team**. The participation of the Legal counsel, Fraud investigators and/or external auditors may also be considered.

    If the irregularity detected or suspected involves the Compliance Office, the Head of Internal Audit takes on all subsequent responsibilities assigned to the former and directly reports to and gets guidance from the **Audit Committee.**

    iv. Investigations of allegations involving senior management or any board member should be overseen by the Board through the Audit Committee and the **legal counsel may be appointed to supervise the investigation**.

2. ***Conducting the Investigation*.** The assigned Investigation team should document and track the steps of investigation, including:
    a. Items maintained as privileged or confidential
    b. Requests for documents, electronic data and other information
    c. Memoranda of Interviews conducted
    d. Analysis of data, documents and interviews and conclusions drawn.

3. ***Reporting the Results.*** The Investigation team should report its findings to the party overseeing the investigation, such as Senior Management, Directors or the legal counsel.

    Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order

to avoid damaging the reputation of persons suspected but subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability.

4. ***Corrective Action.*** After the investigation has been completed, the Company determines what action to take in response to the findings. Any action taken should be appropriate under the circumstances, applied consistently to all levels of employees, including senior management, and should be taken only after consultation with individuals responsible for such decisions. Management consultation with legal counsels is strongly recommended before taking disciplinary, civil, or criminal action. The Company should consider the potential impact of its response and the message that it may send to the public, stakeholders and others.

V. Review of Policy

The Compliance Office, in consultation with the Internal Audit Head and Human Resources Head, is responsible for the administration, revision, interpretation and application of this policy. This policy will be reviewed at least every two (2) years or as needed and revised accordingly.

VI. Reporting to the Insurance Commission

The Company submits a copy of this Anti-Fraud Policy to the Insurance Commission and in case of any material change/s, to submit a revised policy within thirty (30) working days from date of approval of such material change.

The Insurance Commission has the right to review this policy and to take administrative action if it fails to comply with the guidelines set. The Commission may require other reasonable modification of the company's Anti-Fraud Policy, or other remedial action if the review or examination reveals a substantial non-compliance with the terms of the company's Anti-Fraud policy.
