Agthia Fraud Risk Policy		
Custodian of the Document: Head of Governance, Risk & Compliance		
Version: 1.0	Issue Date: August 2022	Effective Date: August 2022

Document History		
Version	Date	Amendment
V.1.0	August 2022	First Version

Approvals	
Designation / Body	Date
Board	4th August 2022

Agthia Group
Fraud Risk Policy

Contents

REVISION LIST

Version	Date	Description
1.0	June 2013	First Version
2.0	July 2015	Second Version
3.0	Jan 2018	Third Version
4.0	June 2022	Significant changes in methodology and scales.

1. Definition

Term	Definition
ACFE	Association of Certified Fraud Examiners
Agthia	Agthia Group Companies
ARC	Agthia's Audit & Risk Committee
Board	Agthia's Board of Directors
Company	Agthia Group
Director	Chairman and/or Member of Agthia's Board of Directors
Employee	Agthia's full-time and part-time employees including senior management, as well as any other person that has been issued an Agthia Employee ID number, (including butnot limited to temporary agency staff, interns and/or trainees)
FRA	Fraud risk assessment
Head of Compliance	Agthia's Director of Risk and Governance is responsible for the Compliance Department Reporting administratively to the CEO and functionally to ARC
Inherent Fraud Risk	The level of fraud risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of an incident.
Policy	Agthia Fraud Risk Assessment Policy
Residual Fraud Risk	Fraud risk remains after control as assessment/risk treatment.
SMART criteria	Specific, measurable, achievable, relevant, time-bound
Subsidiary	An entity where Agthia has more than 50% ownership or has management control.

2. Introduction

The Fraud Risk Assessment Policy (hereafter referred to as the "Policy") defines the requirements and responsibilities related to identification of potential fraud risk scenarios, evaluating them, and preparing risk mitigation plans to appropriately address any elevated risks.

This Policy is to be read in conjunction with the other Agthia's compliance policies, including but not limited to the Agthia's Code of Business Conduct, Whistleblower Policy, and entertainment and gift policy.

Agthia Group defines "Fraud" as a broad concept that refers generally to any intentional act committed to secure an unfair or unlawful gain, which is detrimental to the Group or any of its subsidiaries. Fraud includes any other acts/omissions defined as Fraud as per the applicable laws and regulations in relevant jurisdictions in which Group operates. For this policy, any reference to the term fraud collectively refers to the fraud, corruption and misconduct, as follows:

- Fraud: Deliberate deception to commit, facilitate and/or conceal the misappropriation of assets. It also includes a misrepresentation of statements which encompasses the deliberate manipulation of items in reports and statements, both financial and non-financial.
- Corruption: Breach of trust in the performance of official duties. (e.g. bribery, kickbacks, economic extortion)
- Misconduct: Violations of law, regulations, and internal policies with an intent to secure unlawful gain (e.g. conflicts of interest, insider trading, and anti-competitive practices).

Note: Oversight in relation to laws, regulation, and internal policies without an intent to secure an unlawful gains are not considered fraud. However, such matters shall be addressed as per relevant internal policies.

Actions constituting fraud may mean many things and include (but are not limited to):

- Acceptance/ solicitation of bribes or kickbacks.
- Embezzlement, characterized by misappropriation of money or property, and falsification of financial records to cover up an act.
- Diversion to an employee or outsider of a profitable transaction that would normally generate profits for the Group.
- Intentional concealment or misrepresentation of events, transactions, or data (forgery/alteration of original documents)
- Claims submitted for goods or services not actually provided to the Group (billing schemes/payroll schemes)
- Intentional failure to act in circumstances where the action is required by the Group or by law/regulation (omission of an act);
- Unauthorized or illegal use of confidential or proprietary information.
- Unauthorized or illegal manipulation of IT-related assets (e.g., networks or operating systems)
- Trading company stocks based on information that has not been disclosed to the public or divulging such information to others so that they might trade in such company stocks (violation of Insider Trading)

The Group acknowledges that incidences of fraud risk cannot be eliminated. However, the Group prescribes a zero-tolerance approach to dealing with instances of fraud and to ensure that fraud, corruption, and misconduct are denounced/proscribed/discouraged without exception across the Group.

Agthia Group has adopted and implemented several internal control measures to address fraud risk across the Group, some of the key fraud prevention and detection controls are Group policies and guidelines including Group Authority Matrix. Existing policies and procedures are periodically updated, and new policies and procedures are developed, where required to ensure that adequate internal controls are in place in relation to evolving business requirements.

Employees must disclose any conflict of Interest and provide their individual acknowledgment of the Group's Code of Business Conduct Declaration as per frequency and applicability mentioned in the Code of Business Conduct.

The Group has a mechanism defined under the Whistle Blower Policy to enable employees and other relevant stakeholders

to voice concerns internally in response to the event wherein fraud, corruption, or misconduct is suspected or discovered.

Training and seminars on fraud awareness shall be provided to all employees on a regular basis.

2.1 Purpose of the Policy

The Policy is aimed at:

a. supporting Agthia's ethical business culture and facilitating the creation of an effective anti-fraud environment.
b. assigning the general roles and responsibilities related to conducting fraud risk assessments.
c. establishing a framework for assessing and reacting to potential fraud risks.

2.2 Scope of the Policy

The Policy shall apply to Employees of Agthia's group. All Agthia Employees should follow the procedures and actions related to FRA as per this Policy.

If the requirements of the Policy contradict applicable UAE laws and regulations, the UAE laws and regulations shall supersede the requirements of the Policy from the date such laws and regulations become effective.

2.3 Responsibility for implementation and review of the Policy

The Head of Compliance under the guidance of ARC is responsible for implementing the Policy as well as its annual review and any required updates.

3. General rules

3.1 Fraud Risk Assessment

A fraud risk assessment is a process aimed at proactively addressing an organization's vulnerabilities to both internal and external fraud. The process should allow for the identification of fraud risks that exist or may appear in a business and drive appropriate response to prevent it from materializing and/or mitigate its effects.

3.2 Frequency of performing FRAs

Agthia conducts its FRA on an annual basis.

3.3 Key roles and responsibilities

Agthia's Compliance Department will organize the annual FRA, including obtaining input from Employees, documenting the FRA results, and sharing them with the relevant Agthia stakeholders. Following the FRA, the Compliance Department will be responsible for follow-up on the agreed action plans with the assigned Employees.

All Agthia Employees, Agthia's function/department leaders, will support Agthia Compliance with effective execution of the FRA. This will include indicating and following action plans aimed at mitigating the FRA risks.

The Head of Compliance will ensure that the summary of FRA results is presented to the ARC, in line with the ARC charter.

4. Fraud Risk Governance (Roles and Responsibilities)

4.1 Board of Directors

The Board of Directors has other overall responsibility to set the tone at the top, as outlined in the Board of Directors Charter, to ensure that an effective internal control framework is in place for the Group.

4.2 Audit & Risk Committee

The Audit Committee as outlined in the Audit Committee Charter shall evaluate the adequacy, effectiveness, and efficiency of internal controls to assist the Board in ensuring that the Board is performing its duties in establishing an effective internal control system.

Audit Committee also has the specific responsibility to establish a whistleblowing mechanism for the Group and oversee the investigation of fraud cases including reviewing fraud investigation reports and approving recommendations made.

Oversee the compliance function which is responsible for responding to fraud. Audit Committee also has the authority to investigate or commission an external agency to investigate any cases or allegations of fraud, ethical misconduct, and other irregularities against any person in the Group and its partners. The Committee's detailed responsibilities are set out in the Audit Committee Charter approved by the Board of directors. The ARC reviews FRM assessments and makes recommendations on control gaps to the Board

4.3 Risk and Governance Function

Responsible to ensure the implementation of this policy. Govern the process of fraud risk management. The Group's Risk and Governance Function is responsible for facilitating the Fraud Risk Management (FRM) process across the Group. Also responsible for maintaining the record of fraud cases.

4.4 Conduct and Values Committee

The Conduct and Values Committee (CVC) is appointed as a sub-committee of the Audit Committee by the Board of Directors. The Committee is responsible for receiving, reviewing, assessing the credibility of, and investigating fraud allegations. The Committee's responsibilities are set out in the CVC Charter approved by Audit Committee.

4.5 Senior Executives and Management

The Group positions fraud risk management as an integrated line management function whereby managing and mitigating risks associated with business activities is the responsibility of each employee. They are responsible for detecting fraud or related dishonest activities in their areas of responsibility.

Regularly and systematically assess the potential within their area of responsibility for breaches of integrity, including theft, corruption, and fraud to ensure that relevant fraud prevention procedures are being followed and are effective.

Lead by example to create a culture that encourages open and honest communication; and where it is clear that fraud is not tolerated, any such behavior is dealt with immediately and decisively.

4.6 Internal Control Department

The Internal Control Department is responsible to provide assistance to CVC (whenever requested) in performing the required investigation of suspected fraudulent activities within the Group and accordingly, reporting to the CVC and compliance function and Group Management (where appropriate) on the results and control improvements.

4.7 Employees

All the employees shall adhere to the established Group policies and procedures as well as the Group's Authority Matrix, in their respective areas of work, and also have a basic understanding of fraud and be aware of the red flags.

Report immediately to CVC if they detect any evidence of irregular or improper behaviourbehaviorcted fraud instance may have occurred.

Individual employees shall assist by active involvement in prevention and detection processes, reminding work colleagues of the values of the Group, and reporting cases where fraud, corruption, or abuse of office is suspected. Whistle-blower Policy PP 1038 is intended to encourage and enable employees and others to raise serious concerns within the Group.

4.8 Legal Function

Provide legal guidance to the Investigation Team. Provide advice on the legal position in case of pursuing the accused individual(s) to recover assets stolen or a breach of trust for damages.

5. Conducting the FRA

A fraud risk assessment will have the following four stages:

- Stage 1: Definition of the FRA universe
- Stage 2: Initial identification of potential fraud scenarios
- Stage 3: Assessment of Inherent Fraud Risks and controls
- Stage 4: Response to Residual Fraud Risks

5.1 Stage 1: Definition of the FRA universe

In this stage Agthia's Compliance Department will:

a. Establish the scope of business processes / areas to be covered by the FRA. Its completeness may be additionally verified using Agthia's internal audit universe and/or ERM coverage.
b. Identify the key personnel representing each process / area within the FRA scope.
c. Review the results of earlier FRAs and any past fraud incidents.
d. Create an FRA schedule, including setting interviews with key stakeholders.
e. Prepare a template FRA register to capture the results of the process. A typical FRA register template may list: the covered processes/areas; fraud scenarios for each process/area; assessment of the Inherent Fraud Risk for each scenario, summary of applicable key controls, assessment of key controls effectiveness, assessment of Residual Fraud Risk for each scenario, and ultimately, action plans addressing the elevated risk areas.

Stage 1 output:

- List of processes/areas in scope of the FRA along with key personnel representing each process/area
- FRA schedule of interviews
- Template FRA register

5.2 Stage 2: Initial identification of potential fraud scenarios

In this stage compliance champions, supported by the head of key Agthia functions and departments, will:

a. Initially identify and list the potential/hypothetical fraud scenarios in each of the assessed processes /areas in the earlier prepared FRA register.
b. Verify the completeness of listed fraud scenarios using mapping of the list to the ACFE Fraud Tree (Appendix 1) as applicable for Agthia. This may be supported by additional procedures (if and as required), for example:
    - references to any earlier conducted fraud risk assessments,
    - review of any historical fraud instances, or,
    - available resources related to relevant industry risks and trends.

Stage 2 output:

- FRA Register (list of processes/areas and related fraud scenarios)
- ACFE Fraud Tree completeness review results

5.3 Stage 3: Assessment of Inherent Fraud Risks and controls

In this stage Agthia's Compliance champion, supported by head of key Agthia functions and departments, will:

a. Analyze the listed fraud scenarios with each process/area owner to:
    - confirm, modify, add, or delete the fraud scenarios as appropriate;
    - assess the probability/frequency and impact for each scenario (in line with Appendix 2);
    - calculate the Inherent Fraud Risk for each scenario (in line with Appendix 3, step 1).
b. Identify key controls addressing each of the listed scenarios (Inherent Fraud Risks) and assess their effectiveness together with the process/area owners (in line with Appendix 3, step 2).
c. Calculate and map the Residual Fraud Risk (in line with Appendix 3, steps 3 and 4).

Stage 3 output:

- Update of the FRA Register (reconfirmed list of fraud scenarios, assessed Inherent Fraud Risks for each scenario, list of assessed controls for each fraud scenario, assessed Residual Fraud Risks for each scenario).

5.4 Stage 4: Response to Fraud Risks

In this stage Agthia's Compliance champion, supported by representatives of key Agthia functions and departments, will:

a. Review the list of all Residual Fraud Risks and agree on management actions with the responsible processowners to address each of the risks as below:
    - Management actions, aimed at reducing the Residual Fraud Risks, must be identified for each and every Residual Fraud Risk assessed as Medium or higher.
    - Every Residual Fraud Risk assessed as Very High must be addressed with a high priority action, resolving, or reducing the risk as soon as possible.

- Each management action must meet SMART criteria, including a description of the anticipated steps, identification of the action owner and deadline.

b. Prepare a presentation of the FRA results, including the key management action plans, to the ARC.

Stage 4 output:

- Update of the FRA Register (including the agreed management actions plans)
- FRA summary presentation for the ARC

6. Monitoring of the Residual Fraud Risks management actions

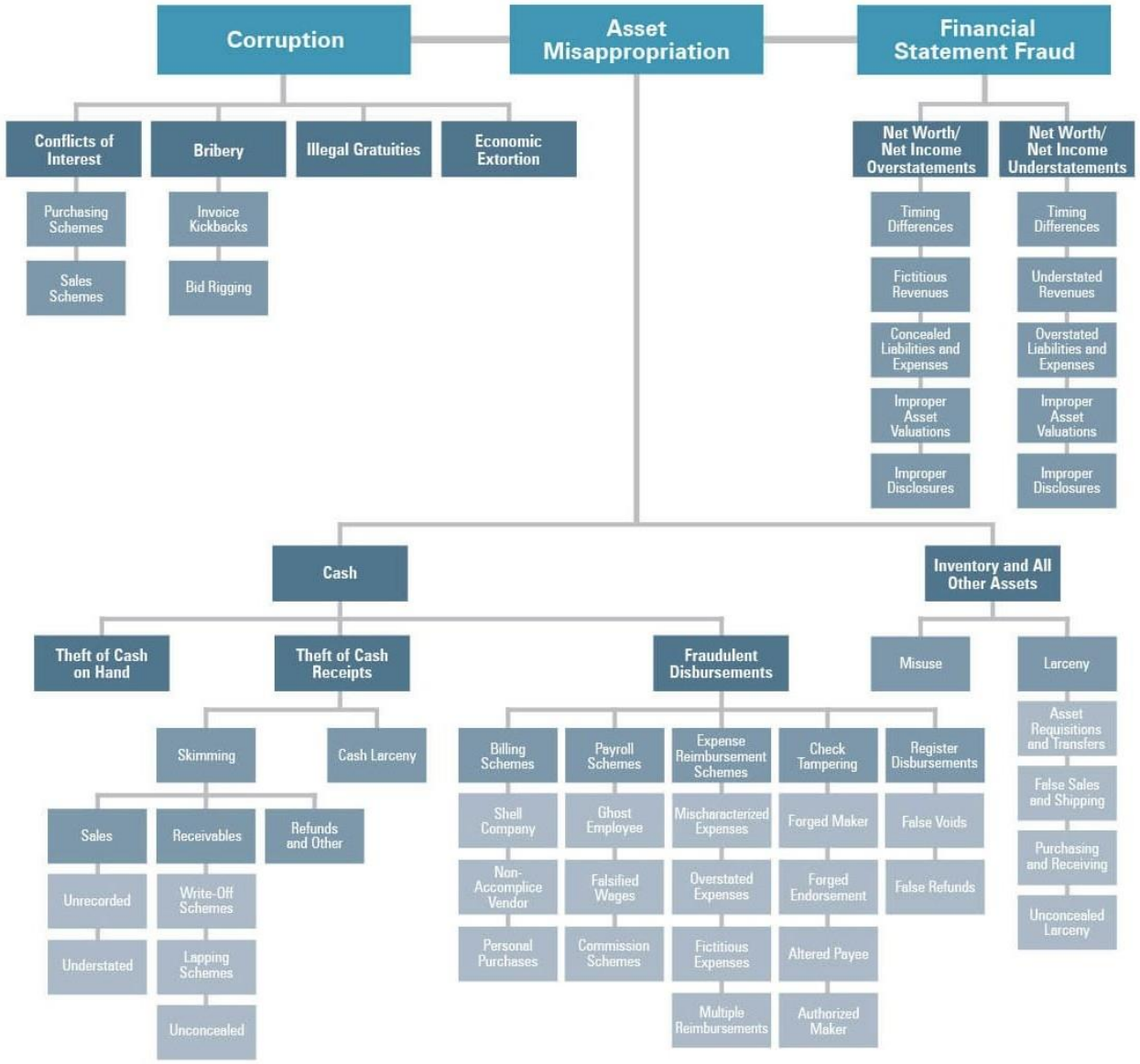
Agthia's Compliance Department will periodically monitor the status of management actions with the relevant process owners. Any unjustified delays may be escalated to the higher-level management / ARC (as appropriate).

Consecutive FRAs should also include a review of the status of any earlier agreed management action plans.

In the event that any fraud is suspected or discovered, the matter should be immediately notified to all members of the Conduct and Values Committee. In cases where suspected irregularity may involve a CVC member, the matter should be notified to Audit Committee (AC).

APPENDICES

Appendix 1 – ACFE Fraud Tree



Appendix 2 – Risk assessment definitions

Likelihood rating definition

Rating	Qualitative Measures	Frequency Measures
Almost Certain 5	Event will occur in most circumstances	90% percent chance of occurrence Occurred or expected to occur more than twenty times a year.
Likely 4	Event will probably occur in most circumstances	65% to 90% chanceof occurrence Occurred or expected to occur more than 12 times a year.
Possible 3	Event should occur in some circumstances	35% to 65% chanceof occurrence Occurred or expected to occur between 6 to 12 times a year.
Unlikely 2	Event could occur in some circumstances	10% to 35% chance of occurrence Occurred or expected to occur between 2 to 5 times a year.
Rare 1	Event may occur in some exceptional circumstances	<10% chance ofoccurrence Occurred or expected to occur less than one time a year.

Rating	Impact Measures			
	Reputational	Financial	Operational	Compliance
Catastrophic 5	• International, long-term media coverage	• Above AED 50 million	• Loss of operations capacity for more than 48 hours	• Non-compliance with laws and regulations resulting in operational restrictions/seizures, financial penalties, or regulatory warning/reprimands; or • Non-compliance with internal policies or contractual agreements resulting in the the significant financial loss (e.g. credit/procurement/food safety policy)
Significant 4	• Significant reputational exposure/ loss with key stakeholders including regulators, financial markets, or shareholders	• Between AED 5,000,001 and AED 4,999,999	• Loss of operations capacity between 47 hours to 12 hours	• Non-compliance with laws and regulations resulting in operations delays, financial penalties, or regulatory orders requiring rectifications; or • Non-compliance with internal policies or contractual agreements resulting in major financial losses (e.g. accounting and reporting/security)
Medium 3	• Reputational exposure to external relationships with suppliers and customers; or • Inability to deliver on strategic initiatives	• Between AED 500,001 and AED 5,000,000	• Loss of operations capacity between 12 hours to 7 hours	• Non-compliance with laws and regulations resulting in operations inefficiencies or conditional regulatory approvals; or • Multiple and/or recurring instances of non-compliance with internal policies or contractual agreements resulting in financial losses or operational delays
Minor 2	• Reputational issue managed by within Agthia; or • Results/ Outcomes from strategic initiatives below expectatpost-implementationation	• Between AED 10,001 and AED 500,000	• Loss of operations capacity between 6 hours to 2 hours	• Isolated instances of non-compliance with internal policies or contractual agreements resulting in some financial losses or operational delays; or
Minor 1	• Not applicable as strategic risks are expected to have at least a moderate impact – refer to other criteria for risks with minor impact	• Up to AED 10,000	• Loss of operations capacity up to 2 hours	• Isolated instances of non-compliance with internal policies or contractual agreements resulting in operational inefficiencies/delays without any direct financial loss

Appendix 3 – Fraud risk calculation

The residual risk level is calculated by conductingthe following steps:

1) Calculate the inherent risk level through the following equation[1]:

   Likelihood rating X Impact rating

   The resulting inherent risk level can be mapped through the following table.

Inherent Risk Level	
Inherent Risk Rating	**Description**
20><=25	Very High
15><=20	High
10><=15	Medium
5><=10	Low
0><=5	Very Low

2) Rate the effectiveness and efficiency of the existing control(s) according to the following rating matrix.

Control Risk Rating	
Control Risk Rating	**Description**
5	Excellent (reduces 81–100% of the risk)
4	Good (reduces 61–80% of the risk)
3	Fair (reduces 41–60% of the risk)
2	Poor (reduces 21–40% of the risk)
1	Unsatisfactory (reduces 0–20% of the risk)

3) Calculate the residual risk level through the following equation:

   Inherent Risk Rating ÷ Control Risk Rating

4) Map the resulting residual risk level according to the following matrix.

Residual Risk Level	
Residual Risk Rating	**Description**
20><=25	Very High
15><=20	High
10><=15	Medium
5><=10	Low
0><=5	Very Low

[1] Refer to **Appendix 2** for rating the likelihood and impact of the identified fraud risks