البنك المركزي السعودي
SAMA
Saudi Central Bank

تعميم

السادة/ المحترمون

السلام عليكم ورحمة الله وبركاته،

الموضوع: تحديث دليل مكافحة الاحتيال المالي.

انطلاقاً من دور البنك المركزي السعودي الإشرافي والرقابي، وحرصاً منه على تعزيز حماية القطاع المصرفي والمتعاملين معه من التعرض لعمليات الاحتيال المالي والأساليب الاحتيالية، واستناداً الى الصلاحيات المنوطة به بموجب نظامه الصادر بالمرسوم الملكي رقم (م/٣٦) وتاريخ ١٤٤٢/٤/١١هـ، والأنظمة الأخرى ذات العلاقة.

مرافق الإصدار المحدث لدليل مكافحة الاحتيال المالي (Counter Fraud Framework)، والذي يهدف إلى تحسين مستوى الممارسات في مكافحة الاحتيال وذلك من خلال تطبيق مجموعة من الضوابط التي تساهم في رفع مستوى النضج لمكافحة الاحتيال بشكل استباقي وأكثر فاعلية للحد من مخاطر الاحتيال، ويتعين على البنوك والمصارف العاملة في المملكة الالتزام بما ورد فيه وفق الإجراءات الآتية:

١. عمل تقييم دقيق للوضع الحالي لإجراءات مكافحة الاحتيال مقارنةً بما ورد في دليل مكافحة الاحتيال المالي (Gap Assessment)؛ لتحديد مواطن الضعف في البنك/ المصرف وتقييم مستوى النضج وفق ما ورد في الدليل من تعريف لـ(Maturity Level)، وتزويد البنك المركزي بتقارير شهرية حيالها اعتباراً من تاريخ ٣٠ نوفمبر ٢٠٢٢م.

٢. وضع خطة عمل (Roadmap)؛ لتحقيق درجة النضج الثالث كحد أدنى للضوابط الواردة في دليل مكافحة الاحتيال خلال (٩) أشهر من تاريخه، بعد تقييم الوضع الحالي في بيئة البنك/ المصرف بشكل دقيق وتزويد البنك المركزي بها في موعد أقصاه تاريخ ٣٠ نوفمبر ٢٠٢٢م.

٣. استيفاء موافقة مجلس إدارة البنك/ المصرف على خطة العمل (Roadmap) وسبل الدعم اللازمة لإنفاذها.

٤. يتعين على البنك/ المصرف الالتزام التام بمتطلبات دليل مكافحة الاحتيال المالي في موعد أقصاه تاريخ ٢٩ يونيو ٢٠٢٣م.

٥. إعداد تقرير سنوي مفصّل من إدارة المراجعة الداخلية - ولها الاستعانة ببيوت الخبرة - يوضح مدى الالتزام بمتطلبات دليل مكافحة الاحتيال المالي ابتداءً من نهاية الربع الرابع من عام ٢٠٢٣م.

٦. يتم تزويد البنك المركزي بخطة العمل المشار إليها في البند (٢)، وكذلك التقارير المشار في البند (١) و(٥) إلى البريد الإلكتروني: CRC.compliance@SAMA.GOV.sa .

٧. يحلّ دليل مكافحة الاحتيال المالي المرافق محلّ دليل مكافحة الاحتيال المالي الصادر بموجب التعميم رقم (٤١٠٧١٣١٥) وتاريخ ١٤٤١/١٢/٢٧هـ، وذلك ابتداءً من تاريخ ٢٩ يونيو ٢٠٢٣م.

للإحاطة، والعمل بموجبه اعتباراً من تاريخه.

النغيان

وتقبلوا تحياتي،

مروان

يزيد بن أحمد آل الشيخ

وكيل المحافظ للرقابة

نطاق التوزيع:

- البنوك والمصارف العاملة في المملكة:

(البنوك المحلية، فروع البنوك الأجنبية، البنوك الرقمية).

Counter-Fraud Framework
Saudi Central Bank

October 2022

Version 1.0

البنك المركزي السعودي
SAMA
Saudi Central Bank

Table of Contents

1. Introduction

1.1. Introduction to the Framework

The advancement of technology has brought rapid changes in the financial sector. While allowing customers instant access to products and services, this digital transformation has increased their vulnerability to fraud. Small scale incidents impacting individuals have been replaced by large scale cyber-enabled fraud attacks orchestrated by international organised groups. These attacks expose customers to ever more sophisticated threats and it is vital that financial institutions properly safeguard assets and mitigate the risk of customers being exploited. Fraud not only causes emotional harm and financial losses to customers, it can also damage the reputation and financial health of organisations, reducing confidence in the overall financial sector in the Kingdom of Saudi Arabia.

The financial sector recognises the rate at which fraud risks are evolving and the importance of controls to prevent, detect and respond to suspected fraud. Delivering an effective approach to fraud risk management will help the Kingdom of Saudi Arabia achieve the 2030 Vision aim to build a stable, thriving, and diversified business environment while protecting members of society and making the Kingdom an unattractive place for fraudsters.

The Saudi Central Bank ("SAMA") has established a Counter-Fraud Framework ("the Framework") to enable organisations it regulates ("the Member Organisations") to effectively identify and address risks related to fraud. The objectives of the Framework are as follows:

1. To create a common approach for addressing fraud risks within the Member Organisations.
2. To achieve an appropriate maturity level of fraud controls within the Member Organisations.
3. To ensure fraud risks are properly managed throughout the Member Organisations.

The Framework will be used to periodically assess the maturity level and evaluate the effectiveness of the Counter-Fraud controls at Member Organisations. The Framework is based on SAMA requirements and industry fraud standards.

1.2. Definition of Fraud

Fraud is defined as any intentional act that aims to obtain an unlawful benefit or cause loss to another party. This can be caused by exploiting technical or documentary means, relationships or social means, using functional powers, or deliberately neglecting or exploiting weaknesses in systems or standards, directly or indirectly.

To support the definition of fraud, Member Organisations should take note of the non-exhaustive list of fraud types included in the Appendix.

1.3. Scope

The Framework defines Principles and Control Requirements for initiating, implementing, maintaining, monitoring, and improving Counter-Fraud controls within Member Organisations regulated by SAMA. The Principles and Control Requirements span the prevention, detection, and response to fraud, as well as the governance of an organisation’s Counter-Fraud Programme. The Framework should be implemented in conjunction with other SAMA frameworks, in particular SAMA’s Cyber Security Framework (“The Cyber Security Framework”), which should be referred to for specific Cyber Security related requirements.

1.4. Applicability

The Framework is applicable to all Member Organisations operating in Saudi Arabia based on SAMA discretion. Member Organisations required to implement and comply with the Framework will be notified by SAMA.

1.5. Responsibilities

The Framework is mandated by SAMA and will be circulated to Member Organisations for implementation. SAMA is the owner and is responsible for periodically updating the Framework. The Member Organisations are responsible for implementing and complying with the Framework.

1.6. Interpretation

SAMA, as the owner of the Framework, is solely responsible for providing interpretations of the Principles and Control Requirements, if required.

1.7. Target Audience

The Framework is intended for Senior and Executive Management, business owners, members of the Member Organisation’s Counter-Fraud Department and those who are responsible for, and involved in planning, defining, implementing, and reviewing Counter-Fraud controls across the three lines of defence.

1.8. Review, Updates and Maintenance

SAMA will review the Framework periodically to determine the Framework’s effectiveness, including the effectiveness of the Framework to address emerging fraud threats and risks. If applicable, SAMA will update the Framework based on the outcome of the review.

If a Member Organisation considers that an update to the Framework is required, the Member Organisation should formally submit the requested update to SAMA. SAMA will review the requested update, and if applicable, the Framework will be adjusted on the next updated version. The Member Organisation will remain responsible to be compliant with the Framework pending the version update.

Please refer to ‘Appendix C – How to request an Update to the Framework’ for the process of requesting an update to the Framework.

Version control will be implemented for maintaining the Framework. Whenever any changes are made, the preceding version shall be retired and the new version shall be published and communicated to all Member Organisations. For the convenience of the Member Organisations, changes to the Framework shall be clearly indicated.

1.9. Reading Guide

The Framework is structured as follows. Chapter 2 elaborates on the structure of the Framework and provides instructions on how to apply the Framework. Chapters 3 to 6 present the actual Framework, including the Counter-Fraud domains and sub-domains, Principles, and Control Requirements.

2. Framework Structure and Features

2.1. Structure

The Framework is structured around four main domains, namely:

- Governance
- Prevent
- Detect
- Respond

For each domain, several sub-domains are defined. A sub-domain focuses on a specific Counter-Fraud topic. Where it is helpful to further delineate Control Requirements, a sub-domain is split into sub-sectors. Per sub-domain (or sub-section), the Framework states a Principle and related Control Requirements.

- A **Principle** summarises the main set of Counter-Fraud controls related to the sub-domain (or sub-section).
- The **Control Requirements** reflect the mandated Counter-Fraud controls that should be considered by Member Organisations when designing and implementing a Counter-Fraud Programme.

The Framework should be implemented in view of the sub-domains' Principles along with its associated Control Requirements.

Control Requirements have been uniquely numbered according to the following numbering system throughout the Framework:

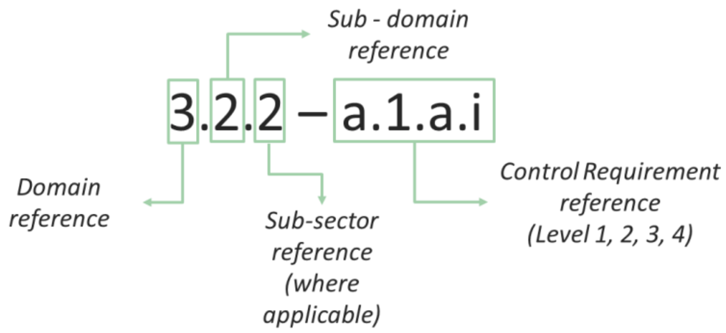

Sub - domain reference
3.2.2 – a.1.a.i
Domain reference
Sub-sector reference (where applicable)
Control Requirement reference (Level 1, 2, 3, 4)

Figure 1 – Control Requirements Numbering System

The figure below illustrates the overall structure of the Framework and indicates the Counter-Fraud Framework domains, sub-domains, and sub-sectors, including a reference to the applicable section of the Framework.

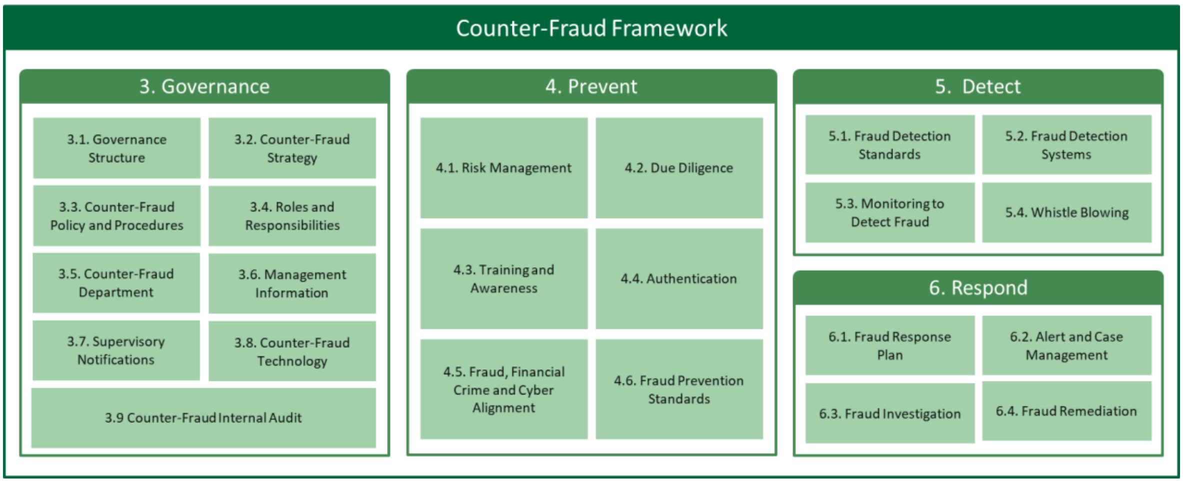

Counter-Fraud Framework
3. Governance
3.1. Governance Structure
3.2. Counter-Fraud Strategy
3.3. Counter-Fraud Policy and Procedures
3.4. Roles and Responsibilities
3.5. Counter-Fraud Department
3.6. Management Information
3.7. Supervisory Notifications
3.8. Counter-Fraud Technology
3.9 Counter-Fraud Internal Audit
4. Prevent
4.1. Risk Management
4.2. Due Diligence
4.3. Training and Awareness
4.4. Authentication
4.5. Fraud, Financial Crime and Cyber Alignment
4.6. Fraud Prevention Standards
5. Detect
5.1. Fraud Detection Standards
5.2. Fraud Detection Systems
5.3. Monitoring to Detect Fraud
5.4. Whistle Blowing
6. Respond
6.1. Fraud Response Plan
6.2. Alert and Case Management
6.3. Fraud Investigation
6.4. Fraud Remediation

Figure 2 – Counter-Fraud Framework Structure

To aid consistency of implementation in Member Organisations, Appendix A contains a glossary of defined terms. Where a defined term is used in the domains and sub-domains in Chapters 3 to 6, it is included in italicised text (e.g., internal fraud, Fraud Risk Assessment, Intelligence Monitoring etc.).

2.2. Principle-Based

The Framework is principle-based, supported by a specific set of Control Requirements, allowing Member Organisations to adopt a risk-based approach within the applicable laws of the KSA. This means that it prescribes key Counter-Fraud principles to be embedded and achieved by the Member Organisations. The list of mandated Control Requirements provides additional direction and should be considered by Member Organisations. When a certain Control Requirement cannot be implemented, the Member Organisation should follow an exception process involving the consideration of compensating controls proportionate to business operations, pursuing an internal risk acceptance and finally requesting a formal waiver from SAMA. Approval of waiver requests will be at the discretion of SAMA. Please refer to Appendix E for details for the – How to request a Waiver from the Framework – process.

2.3. Self-Assessment, Review and Audit

The implementation of the Framework at the Member Organisations will be subject to a periodic self-assessment. The self-assessment will be performed by the Member Organisations based on a questionnaire. The self-assessments will be reviewed and audited by SAMA to determine the level of compliance with the Framework and the Counter-Fraud maturity level of the Member Organisations. Please refer to ’2.4 Counter-Fraud Maturity Model’ for more details about the Counter-Fraud Maturity Model.

2.4. Counter-Fraud Maturity Model

The Counter-Fraud maturity level will be measured with the help of a predefined maturity model. The Counter-Fraud Maturity Model distinguishes 6 maturity levels (0, 1, 2, 3, 4 and 5), which are summarised in the table below. In order to achieve levels 3, 4 or 5, Member Organisations should first meet all criteria of the preceding maturity levels.

Maturity Level	Definition and Criteria	Explanation
0 Non-existent	• No documentation. • There is no awareness or attention for certain Counter-Fraud controls.	• Counter-Fraud controls are not in place. There may be no awareness of the particular risk area or no current plans to implement such Counter-Fraud controls.
1 Ad-hoc	• Counter-Fraud controls are not or partially defined. • Counter-Fraud controls are performed in an inconsistent way. • Counter-Fraud controls are not fully defined.	• Counter-Fraud control design and execution varies by department or owner. • Counter-Fraud control design may only partially mitigate the identified risk and execution may be inconsistent.
2 Repeatable but informal	• The execution of the Counter-Fraud controls is based on an informal and unwritten, though standardised, practice.	• Repeatable Counter-Fraud controls are in place. However, the control objectives and design are not formally defined or approved. • There is limited consideration for a structured review or testing of a control.
3 Structured and formalised	• Counter-Fraud controls are defined, approved, and implemented in a structured and formalised way. • Fraud detection system capability is implemented and embedded. • The implementation of Counter-Fraud controls can be demonstrated. • Reporting is in place to monitor Counter-Fraud control performance.	• Counter-Fraud policies, standards and procedures are established • Counter-Fraud controls are implemented and embedded. • Fraud detection system capability is in place to prevent and proactively detect fraud across all products and channels. • Compliance with Counter-Fraud documentation (i.e., policies, standards, and procedures) is monitored, preferably using a governance, risk, and compliance tool (GRC). • Key Performance Indicators are defined and reported to monitor the implementation of controls.
4 Managed and measurable	• The effectiveness of Counter-Fraud controls is periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of implemented Counter-Fraud controls is measured and periodically evaluated. • Key Risk Indicators and trend reporting are used to monitor position against risk appetite and give an early warning of potential emerging issues. • Results of measurement and evaluation are used to identify opportunities for improvement of the Counter-Fraud controls.
5 Adaptive	• Counter-Fraud controls are subject to a continuous improvement plan.	• The enterprise-wide Counter-Fraud Programme focuses on continuous compliance, effectiveness, and improvement of the Counter-Fraud controls.

		- Counter-Fraud controls are integrated with enterprise risk management framework and practices.

Table 1 – Counter-Fraud Maturity Model

The objective of the Framework is to create an effective approach for addressing and managing Counter-Fraud risks within the financial sector. To achieve an appropriate Counter-Fraud maturity level, the Member Organisations should at least operate at maturity level 3 or higher as explained below.

2.4.1. Maturity Level 3

To achieve level 3 maturity, a Member Organisation should define, approve, and implement Counter-Fraud controls in line with the Control Requirements of this Framework. This includes the implementation of fraud detection system capability to prevent and proactively detect fraud.

In addition, a Member Organisation should monitor compliance with the Counter-Fraud documentation. The Counter-Fraud documentation should clearly indicate "why", "what" and "how" Counter-Fraud controls should be implemented. The Counter-Fraud documentation consists of Counter-Fraud policies, standards, and procedures.

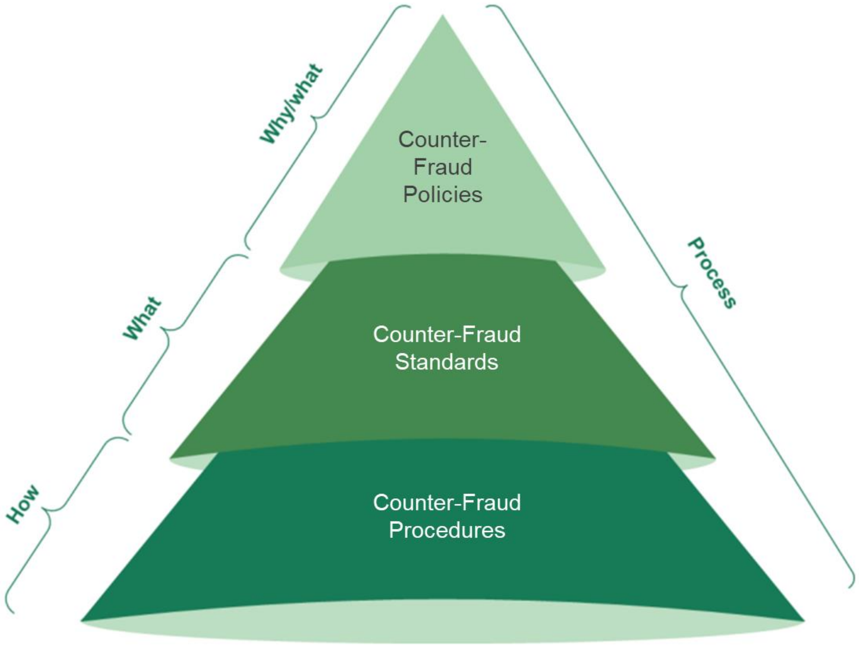


Figure 3 - Counter-Fraud Documentation Pyramid

The Counter-Fraud Policy should be endorsed and mandated by the Board of the Member Organisation and state "why" countering fraud and protecting customers is important to the Member Organisation. The policy should highlight the overall scope of the Counter-Fraud

Programme, key Counter-Fraud responsibilities and “what” Counter-Fraud principles and objectives should be established.

Based on the Counter-Fraud Policy, Counter-Fraud standards should be developed. These standards define “what” Counter-Fraud controls should be implemented, such as, Due Diligence, authentication, prevention, and detection etc. The standards support and reinforce the Counter-Fraud Policy and are to be considered as Counter-Fraud baselines.

The step-by-step tasks and activities that should be performed by staff of the Member Organisation are detailed in the Counter-Fraud procedures. These procedures prescribe “how” the Counter-Fraud controls, tasks and activities have to be executed in the operating environment.

The actual progress of the implementation, performance and compliance of the Counter-Fraud controls should be periodically monitored using Key Performance Indicators (KPIs).

2.4.2. Maturity Level 4

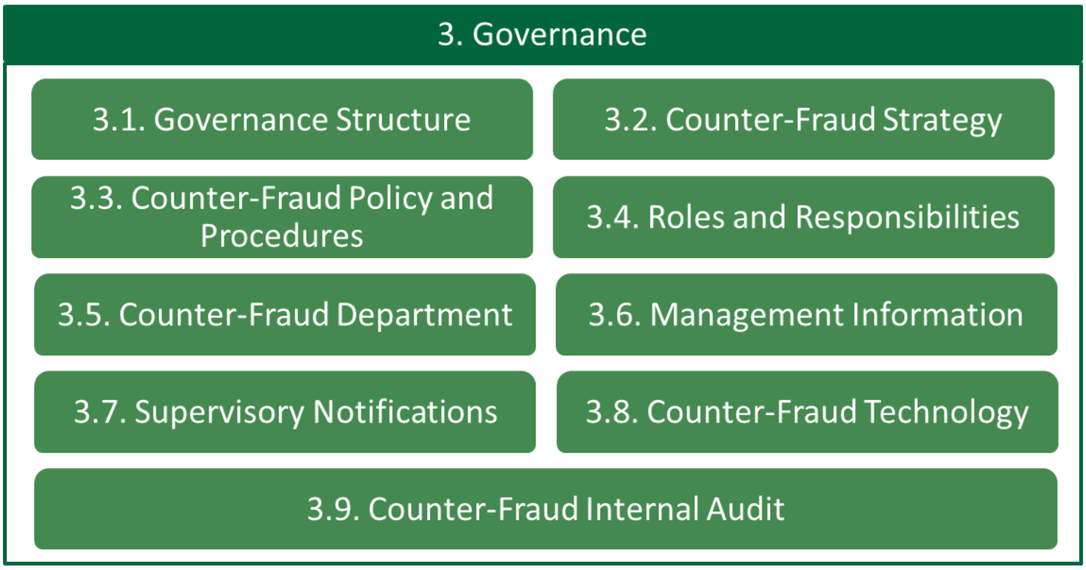
To achieve maturity level 4, Member Organisations should periodically measure and evaluate the effectiveness of the Counter-Fraud controls implemented to achieve maturity level 3. In order to measure and evaluate whether the Counter-Fraud controls are effective, Key Risk Indicators (KRIs) should be defined. A KRI indicates the norm for effectiveness measurement and should define thresholds to determine whether the actual result of measurement is below, on, or above the targeted norm. KRIs are used to monitor a potential increase in fraud risk exposure and allow actions to be taken to mitigate the risk before an increase in fraud cases occurs.

2.4.3. Maturity Level 5

Maturity level 5 focuses on the continuous improvement of Counter-Fraud controls. Continuous improvement is achieved through continuously analysing the goals and achievements of Counter-Fraud governance and identifying structural improvements. Counter-Fraud controls should be integrated with enterprise risk management practices and supported with automated real-time monitoring to assess control effectiveness. Business process owners should be accountable for monitoring the compliance of the Counter-Fraud controls, measuring the effectiveness of the Counter-Fraud controls, and incorporating the Counter-Fraud controls within the enterprise risk management framework.

3. Governance

The Board and Executive Leadership of the Member Organisation is ultimately responsible for creation of a *Counter-Fraud Programme*; providing leadership and direction; and projecting a *Counter-Fraud culture* inside and outside the organisation. The programme should include a *Counter-Fraud Strategy* to define organisational objectives, a *Counter-Fraud Policy* outlining responsibilities and mandatory requirements, and a Governance Structure with associated internal and external reporting aligned to the organisation's size and complexity to monitor and oversee *fraud risk management*.



3. Governance

3.1. Governance Structure

3.2. Counter-Fraud Strategy

3.3. Counter-Fraud Policy and Procedures

3.4. Roles and Responsibilities

3.5. Counter-Fraud Department

3.6. Management Information

3.7. Supervisory Notifications

3.8. Counter-Fraud Technology

3.9. Counter-Fraud Internal Audit

Figure 4 – Governance Domain

3.1. Governance Structure

Principle

Member Organisations should establish and maintain a *Counter-Fraud Governance* Structure owned by *Senior Management* with responsibility for oversight and control of all aspects of the organisational *Counter-Fraud Programme*.

Control Requirements

a. Member Organisations should establish and maintain a dedicated *Counter-Fraud Governance Committee (CFGC)*.

b. The *CFGC* should be headed by a member of the Executive Committee (e.g., CEO, CRO or equivalent).

c. The following positions at a minimum should be represented in the *CFGC*:

   1. Head of Counter-Fraud/Senior Manager accountable for the *Counter-Fraud Programme*.
   2. Chief Risk Officer.
   3. Chief Operating Officer.
   4. Head of Digital.

5. Heads of relevant business departments or product owners (e.g., General Manager of Retail/Corporate).
6. *Senior Managers* from all departments involved in *fraud risk management* (e.g., Operational Risk Management, Cyber Security, *Counter-Fraud Department*, Analytics, Compliance).
7. Internal Audit should attend as an "observer".

d. A *CFGC* charter should be developed, approved, and reflect the following:
    1. Committee objectives.
    2. Authority and accountability of the committee.
    3. Roles and responsibilities.
    4. Minimum number and role of meeting participants required to meet quorum.
    5. Meeting frequency (minimum on a quarterly basis).
    6. Escalation process for fraud issues or incidents to Board level.
    7. Documentation and retention of meeting minutes and decisions.

e. The *CFGC* should at a minimum be responsible for:
    1. Approving, supporting, communicating, and monitoring:
        a. Counter-Fraud Strategy.
        b. Counter-Fraud Policy.
        c. *Fraud Risk Management* Framework that should include at a minimum:
            i. *Intelligence Monitoring* process.
            ii. *Fraud Risk Assessment*.
            iii. *Fraud Risk Appetite*
            iv. *KRIs* for fraud.
        d. *Management Information*
    2. Providing leadership, direction, and oversight of the Member Organisation's *Counter-Fraud Programme*.

f. Member Organisations should appoint an appropriately qualified and experienced Head of Counter-Fraud as accountable for the *Counter-Fraud Programme* at *Senior Management* level (see control requirement 3.5.e).

g. Member Organisations should establish a documented and approved process for Counter-Fraud budget and spending prioritisation which should align with fraud strategic objectives.

h. The overall Counter-Fraud budget should be monitored, reviewed periodically, and adjusted accordingly by the CFGC to meet the Counter-Fraud and business needs.

i. Member Organisations should define roles and responsibilities of *Senior Management* and *Counter-Fraud Department* employees using a responsibility assignment matrix, also known as *RACI*. The *RACI Matrix* should outline who is responsible and accountable for Counter-Fraud processes and controls, as well as who should be consulted or informed.

3.2. Counter-Fraud Strategy

Principle

Member Organisations should define, approve, implement and maintain a *Counter-Fraud Strategy* aligning to the overall strategic objectives of the organisation that identifies short and long-term Counter-Fraud initiatives and communicates a plan of action to achieve them.

Control Requirements

a. *Counter-Fraud Strategy* should be defined, approved, implemented and maintained.

b. Counter-Fraud strategic initiatives should be translated into a defined roadmap including but not limited to, consideration of:
   1. Timescales to deliver initiatives.
   2. The owner responsible for delivering the initiative.
   3. How the initiatives will close the gaps between current and target environments.
   4. The integration of initiatives into a coherent *Counter-Fraud Strategy* that aligns with the business strategy.
   5. Dependencies, overlaps, synergies and impacts among projects, and prioritisation.

c. *Counter-Fraud Strategy* should be aligned with:
   1. The Member Organisation's overall business strategic objectives.
   2. Broader strategies that may influence fraud risks and controls, e.g., *Cyber Security*, IT, *Financial Crime* (Anti-Money Laundering (AML) & Customer *Due Diligence* (CDD)).
   3. Legal and regulatory compliance requirements of the Member Organisation and any other applicable laws in the Kingdom of Saudi Arabia (KSA).

d. *Counter-Fraud Strategy* should at a minimum address:
   1. The current state maturity of the Member Organisation, including the most significant fraud related challenges faced.
   2. The people, process, and technology requirements to deliver the strategy and proactively manage fraud within risk appetite.
   3. The future direction of the Member Organisation's *Counter-Fraud Programme*, and the initiatives required to successfully migrate to the desired future state.
   4. Known changes to the *fraud landscape* (e.g., the increasing digitalisation of financial services products, new external threats, new regulation, or guidance).

e. A Member Organisation should review and when required update its *Counter-Fraud Strategy* on a periodic basis or whenever there is a material change:
   1. Internally (e.g., the Member Organisation's business model, operational environment, or business strategy).
   2. Externally (e.g., the *fraud landscape* or applicable laws and regulations).

3.3. Counter-Fraud Policy and Procedures

Principle

Member Organisations should define, approve, communicate, and implement a *Counter-Fraud Policy* to set the commitment and objectives for Counter-Fraud and provide requirements to relevant stakeholders; and associated procedures to outline the step-by-step tasks and activities that should be performed by employees.

Control Requirements

a. *Counter-Fraud Policy* and procedures should be defined, approved, communicated and implemented.

b. *Counter-Fraud Policy* and procedures should take into consideration the risks identified in the *Fraud Risk Assessment*, the evolving *fraud landscape* and the Member Organisation's business model and operations, and should be periodically reviewed to ensure the identified risks are managed effectively.

c. *Counter-Fraud Policy* should be readily accessible to all employees, *contractors* and relevant *third parties*, including all branches and majority-owned subsidiaries.

d. *Counter-Fraud Policy* should require Member Organisations to follow all applicable Counter-Fraud laws and regulations, and payment operator requirements.

e. *Counter-Fraud Policy* should include at a minimum, the following:
   1. A defined owner of appropriate seniority and role (e.g., Head of Counter-Fraud).
   2. The Member Organisation's overall fraud objectives and scope.
   3. A statement of the Board's intent, supporting the fraud objectives.
   4. Core requirements to provide a consistent, proportionate, and effective approach to the management of fraud risk.
   5. Responsibilities for key stakeholders and relevant *third parties* who play a role in fraud governance, prevention, detection, or response across the three lines of defence (e.g., *Senior Management*, Compliance, Internal Audit).
   6. Escalation and reporting requirements in the event of a *policy breach*.

f. Counter-Fraud procedures should outline the step-by-step tasks and activities that should be performed by employees in the operating environment for Counter-Fraud process and control operation (e.g., product risk assessment, alert handling, investigations).

g. For Member Organisations with a headquarters in the KSA, the *Counter-Fraud Policy* should apply across all international branches and subsidiaries. If the law of another jurisdiction prohibits compliance, an exemption should be documented and approved.

3.4. Roles and Responsibilities

Principle

Member Organisations should define, approve and implement Counter-Fraud roles and responsibilities across the three lines of defence and all relevant stakeholders should have an adequate level of understanding of the expectations related to their role.

Control Requirements

a. Member Organisations should define, approve and implement Counter-Fraud roles and responsibilities for all relevant stakeholders and ensure they have been communicated and understood.

b. The Board should be accountable for:
   1. The establishment of a *Counter-Fraud Programme*.
   2. Setting the tone from the top to establish a *Counter-Fraud culture* through a *Code of Conduct* (or equivalent).

3. Ensuring that a robust *Fraud Risk Management* framework is established and maintained to manage fraud risks.
4. Ensuring that sufficient budget for Counter-Fraud is allocated, utilised, and monitored.
5. Approving the *CFGC* charter.
6. Endorsing (after being approved by the *CFGC*):
   a. The roles and responsibilities of *Senior Management* accountable for the *Counter-Fraud Programme.*
   b. The *Counter-Fraud Strategy.*
   c. The *Counter-Fraud Policy*.
   d. The output of the *Fraud Risk Assessment*.
   e. *Fraud Risk Appetite*.

c. The Head of Counter-Fraud should be accountable for:
1. Developing, implementing, and maintaining:
   a. *Counter-Fraud Strategy*.
   b. *Counter-Fraud Policy*.
   c. *Fraud Risk Assessment*.
   d. *Fraud Risk Appetite*.
   e. *KRIs* for fraud.
2. Reinforcing and maintaining the tone from the top to deliver a culture of compliance with the *Code of Conduct*.
3. Developing a risk-based *Counter-Fraud Programme* that addresses people, process, and technology, including adequate systems to prevent, detect and respond to fraud.
4. Ensuring that detailed Counter-Fraud standards and procedures are established, approved, and implemented.
5. Ensuring that Counter-Fraud systems and controls remain effective in light of evolving threats identified through *Intelligence Monitoring*.
6. Periodically informing *CFGC* on the latest developments on Counter-Fraud strategic initiatives and implementation status.
7. Establishing a *Counter-Fraud Department* that is adequately resourced and has responsibility for the requirements outlined in sub-domain 3.5.
8. Collating and overseeing organisation-wide *Management Information* reporting produced in relation to Counter-Fraud risks and performance.
9. Promptly notifying SAMA of new fraud typologies and significant fraud incidents in line with the Supervisory Notification requirements included in sub-domain 3.7.
10. Taking action when a notification is received of any significant fraud incidents, investigations or breaches of Counter-Fraud policy or standards, and reporting to the Board or *CFGC* as required.
11. Defining the organisation's ongoing fraud awareness programme in coordination with relevant departments (e.g., operations, Communications, Human Resources (HR)).

d. At a minimum, *Senior Management* should be accountable for:

1. Ensuring that employees are compliant with the *Code of Conduct* and Counter-Fraud policies, standards, and procedures.
2. Ensuring that employees receive training in line with the requirements of the fraud training and awareness programme.
3. Developing and reviewing regular *Management Information* reporting to monitor Counter-Fraud risks and performance.
4. Notifying the *CFGC* where escalation is required (e.g., adverse internal findings relating to Counter-fraud controls or fraud risk appetite is exceeded).
5. Managing fraud losses through processes and controls in own area of accountability within the organisation's agreed *Fraud Risk Appetite*.
6. Maintaining appropriate systems and controls to prevent, detect and respond to fraud.

e. Manager(s) accountable for fraud operations (e.g., managing fraud alerts, responding to reported fraud and dealing with fraud cases) should be responsible for:
   1. Ensuring that all suspected fraud, including system alerts and manual employee and customer referrals are adequately prioritised, investigated and the outcome is appropriately recorded.
   2. Taking immediate steps to prevent further exposure and corrective action(s) when a fraud is identified.
   3. Notifying relevant external parties (e.g., law enforcement).

f. The Internal Audit function should be responsible for:
   1. The identification of a comprehensive set of auditable areas for fraud risk.
   2. Assessment and prioritisation of fraud risks during audit planning.
   3. Performing fraud audits and producing independent objective reports.

g. All Member Organisation employees should be responsible for:
   1. Complying with applicable Counter-Fraud policies, standards, and procedures.
   2. Reporting any suspicions of fraud in a timely manner.

h. Member Organisations should ensure that suspected or actual cases of *internal fraud* are investigated by individuals of appropriate seniority (e.g., if the fraud involves a manager, an individual of higher seniority should take responsibility for the oversight and approval of the investigation); and independence (e.g., internal audit or an equivalent control function should conduct the investigation with the investigators free from potential conflicts of interest).

i. Member Organisations should periodically review the roles and responsibilities of employees with fraud related responsibilities to ensure they reflect best practice, address trending fraud *typologies* and are aligned with the *fraud landscape* and business model.

j. Member Organisations should develop a formal Counter-Fraud succession plan in coordination with the HR Department taking into consideration the reliance on key Counter-Fraud employees having critical roles and responsibilities.

3.5. Counter-Fraud Department

Principle

Member Organisations should establish and maintain a *Counter-Fraud Department* that has responsibility for the day-to-day operation of the *Counter-Fraud Programme*.

Control Requirements

a. Member Organisations should establish and maintain a *Counter-Fraud Department* that has responsibility for the day-to-day operation of the *Counter-Fraud Programme*, including at a minimum:
   1. Monitoring and overseeing compliance with Counter-Fraud policies, standards, and procedures.
   2. Designing and implementing organisation wide required counter-fraud controls covering people, process and technology dimensions.
   3. Performing an in-depth organisation wide *Fraud Risk Assessment*.
   4. Analysis of Counter-Fraud data and intelligence to proactively identify fraud trends.
   5. Sharing Counter-Fraud Intelligence with SAMA and other organisations in the sector.
   6. Proactively and reactively tuning Counter-Fraud systems.
   7. Monitoring of Counter-Fraud Operations.
   8. Performing comprehensive fraud investigations, identifying root causes of fraud incidents and documenting corrective actions.
   9. Monitoring Fraud Risk Appetite measures and actively engaging a crisis management task force if the defined limit is breached with an impact on customers (see control requirement 4.1.3.d).
   10. Ensuring alignment of Counter-Fraud capabilities with Cyber Security and *Financial Crime*.
   11. Periodic reporting to senior management covering at minimum:
       a. *Fraud Risk Assessment* results.
       b. Fraud typologies identified.
       c. *Fraud Risk Appetite* measures and performance against thresholds and limits.
       d. Operational and customer fraud losses.

b. Member Organisations should assess the most appropriate reporting line for the *Counter-Fraud Department* based on organisational structure; decision making authority; visibility to the Executive Committee/Board; and *Senior Management* accountability and responsibilities.

c. Member Organisations should evaluate the staffing requirements of the *Counter-Fraud Department* on a periodic basis and in response to material changes to the business, operational and *fraud landscape* or the Member Organisation *Fraud Risk Assessment*.

d. Evaluation of staffing requirements should consider both the capacity (number of resources) and the capability (skills and experience) required.

e. The Head of Counter-Fraud should have skills and experience at a minimum consisting of:
   1. An in-depth understanding of fraud risks in the financial sector.
   2. Strong knowledge of digital fraud threats and common typologies, along with emerging trends impacting financial sector organisations and their customers.
   3. Designing and implementing technology and controls based on use-cases to mitigate fraud risks and threats.

4. The use of data and analytics to proactively prevent fraud and protect customers.

f. The *Counter-Fraud Department* should at a minimum include employees with skills and experience in:
   1. Fraud risks and typologies related to the products offered by the organisation (e.g., experience in payment fraud; scams; and social engineering).
   2. Fraud risks and typologies related to the delivery channels offered by the organisation, in particular digital channels such as online and mobile.
   3. Counter-Fraud data analytics to enable the analysis of large volumes of transactions and proactive identification of fraud threats.
   4. Counter-Fraud technology to ensure systems are operating effectively with scenarios relevant to the risks faced by the Member Organisation.
   5. The analysis of intelligence and data to identify fraud trends and the root cause of fraud incidents.
   6. Fraud investigations, from initial notification of a potential incident to closure and corrective actions.
   7. Reporting and production of *Management Information* to monitor organisational fraud performance.

g. Member Organisations should consider fraud qualifications for roles in the *Counter-Fraud Department*.

h. Member Organisations should establish a training plan and provide periodic training to develop and maintain the competency of the employees in the *Counter-Fraud Department*.

i. Where *third party* services or resources (e.g., *contractors* or Managed Services) are used to fulfil responsibilities of the *Counter-Fraud Department*, Member Organisations should ensure the resource is appropriately vetted and monitored.

3.6. Management Information

Principle

Member Organisations should define, approve and implement a process for the reporting of *Management Information* to enable *Senior Management* to monitor Counter-Fraud risks and performance.

Control Requirements

a. Member Organisations should define, approve and implement a process for the reporting of *Management Information* to monitor Counter-Fraud risks and performance.

b. Fraud *Management Information* should be reported to *Senior Management* and the CFGC on a periodic basis and on an ad hoc basis as required (e.g., if a new or unusual typology is identified).

c. Member Organisations should coordinate the collation of fraud *Management Information* to ensure a holistic picture can be reported of all fraud impacting the organisation or its customers.

d. Member Organisations should identify appropriate *Management Information* to adequately inform *Senior Management* of Counter-Fraud risks and performance. At a minimum this should include:
    1. *Fraud Risk Assessment* results.
    2. *Fraud Risk Appetite* measures and performance against thresholds and limits.
    3. Volume of fraud alerts notified by:
        a. Customers
        b. Employees
        c. Fraud systems
    4. Volume and trends of Fraud cases handled, split by product and *typology*.
    5. New *typologies* identified.
    6. Value of *near misses* or potential frauds that were detected and prevented.
    7. Case value of fraud handled (the total value of the fraud case, including actual and potential losses).
    8. Fraud losses, split by product, payment type (where applicable) and *typology*, including:
        a. Customer losses
        b. Operational losses.
    9. Value of customer refunds following fraud.

3.7. Supervisory Notifications

Principle

Member Organisations should immediately notify SAMA of new fraud *typologies* and significant fraud incidents to mitigate the risk of the fraud impacting additional customers, other organisations, or the financial sector in the KSA.

Control Requirements

a. Member Organisations should notify the SAMA General Department of Cyber Risk Control immediately of the following:
    1. Any new *fraudulent typology* whether it resulted in financial loss or not (e.g., type of fraud not previously observed or new *scam* attempt detected).
    2. Where an external person has committed or attempted to commit a significant fraud against it.
    3. Where an employee of a Member Organisation has committed a significant *internal fraud* against one of its customers or may be guilty of serious misconduct concerning honesty or integrity related to the organisation’s regulatory obligations.
    4. Where *Wholesale Payment Endpoint Security* Fraud is suspected or identified.
    5. Where a significant irregularity is identified in the organisation’s accounting records that may be indicative of fraud.

b. When assessing whether a fraud is considered significant to meet the notification requirements above, Member Organisations should consider at a minimum:

1. The value of any monetary loss or potential monetary loss to the organisation or its customers (the value should consider an individual fraud incident or total losses from connected incidents).
2. The number of customers impacted.
3. Reputational damage to the organisation and the wider financial sector.
4. Whether any regulation has been breached.
5. Whether the incident reflects weaknesses in the organisation's Counter-Fraud controls.
6. If the incident has the potential to impact other Member Organisations.

c. Member Organisations should use the standard reporting template in Appendix G to notify SAMA.

d. At a minimum, Member Organisations should include the origin of the incident; the methods used; related parties (internal and external); corrective actions; and losses, if any, in the notification to SAMA. Where all required information is not available at the time of notification, any gaps should be supplied to SAMA promptly as the investigation progresses.

3.8. Counter-Fraud Technology

Principle

Member Organisations should define, approve and implement a strategy for the sourcing or development and implementation of counter-fraud systems and technology to manage the fraud risks they are exposed to.

Control Requirements

a. Member Organisations should define, approve and implement a strategy for the sourcing or development of Counter-Fraud systems and technology to prevent, detect and respond to fraud.

b. Member Organisations should implement Counter-Fraud systems and technology and verify that they are operating as intended.

c. The output of the *Fraud Risk Assessment* should inform the technology required, and systems should be proportionate to the *risk appetite* of the organisation.

d. Whether a fraud system is sourced from a vendor or developed in-house, Member Organisations should consider the below requirements at a minimum:

1. The *Counter-Fraud Department* are engaged in the design and implementation of the system with oversight from the CFGC.
2. The rationale for scenarios developed and thresholds applied is documented.
3. The system and *rules* are designed or can be customised to align to the products, services, and fraud risks of the organisation.
4. New *rules* can be implemented on a timely basis to target prevention and detection of new or emerging typologies identified through *Intelligence Monitoring*.
5. Awareness of *rules* to prevent and detect potential *internal fraud* is limited to a restricted, documented set of roles which does not include employees or *third*

parties responsible for the operation of processes and controls being monitored (e.g., branch/customer facing staff or operational payments teams).

6. Configuration changes should follow the System Change Management Principles and Control Requirements in SAMA's Information Technology Governance Framework ("The IT Governance Framework").
7. The organisation can explain and outline the *fraud threats* that scenarios are designed to monitor and mitigate.
8. Where *Machine Learning* or *Artificial Intelligence* are used the system should not be '*black box*' and should be capable of being audited (e.g., the organisation should have the capability to test what the algorithms are designed to do and whether they are correctly implemented).
9. Business Continuity and IT Disaster Recovery Plans are in place aligned to the requirements of the SAMA Business Continuity Management Framework.

3.9. Counter-Fraud Internal Audits

Principle
Member Organisations should conduct audits in accordance with generally accepted auditing standards and relevant SAMA framework(s) to verify that the fraud control design is adequately implemented and operating as intended.

Control Requirements

a. Member Organisations should ensure that Counter-Fraud audits are performed independently and according to generally accepted auditing standards and relevant SAMA frameworks.

b. Member Organisations should establish an audit cycle that determines the frequency of Counter-Fraud audits.

c. Member Organisations should develop a formal Counter-Fraud audit plan addressing people, process and technology components.

d. The frequency of Counter-Fraud audit should be aligned with the output of the *Fraud Risk Assessment* and consider the criticality and risk of the Counter-Fraud system, control or process.

e. The Internal Audit function of Member Organisations should complete periodic validation of the implementation of Counter-Fraud related corrective actions, including those resulting from SAMA instruction.

f. Member Organisations should ensure that the Counter-Fraud auditors have the requisite level of competencies and skills to effectively assess and evaluate the adequacy of Counter-Fraud policies, procedures, processes and controls implemented.

g. Counter-Fraud audit reports, at a minimum, should:
    1. Include the findings, recommendations, management's response with defined action plan, and responsible party and limitations in scope with respect to the Counter-Fraud audits.
    2. Be signed, dated and distributed according to the format defined.
    3. Be submitted to the audit committee on periodical basis.

h. A follow-up process for audit observations should be established to track and monitor Counter-Fraud audit observations.

4. Prevent

An effective *Counter-Fraud Programme* includes fraud prevention processes and controls to facilitate the identification of threats and mitigate the risk of fraud occurring. These processes and controls are proactive and have the objective of stopping a fraudster acting before they can cause harm to the organisation or its customers.

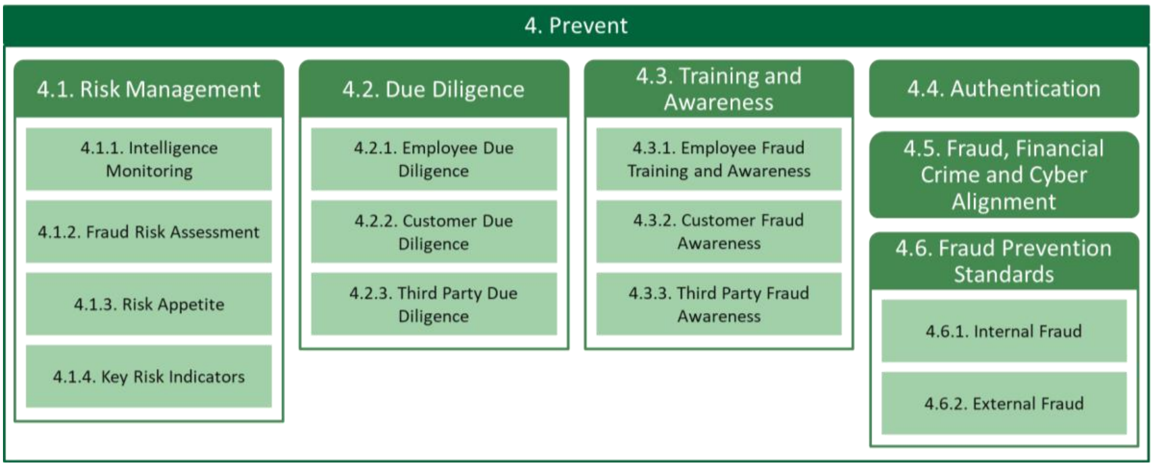

4. Prevent
4.1. Risk Management
4.1.1. Intelligence Monitoring
4.1.2. Fraud Risk Assessment
4.1.3. Risk Appetite
4.1.4. Key Risk Indicators
4.2. Due Diligence
4.2.1. Employee Due Diligence
4.2.2. Customer Due Diligence
4.2.3. Third Party Due Diligence
4.3. Training and Awareness
4.3.1. Employee Fraud Training and Awareness
4.3.2. Customer Fraud Awareness
4.3.3. Third Party Fraud Awareness
4.4. Authentication
4.5. Fraud, Financial Crime and Cyber Alignment
4.6. Fraud Prevention Standards
4.6.1. Internal Fraud
4.6.2. External Fraud

Figure 5 – Prevent Domain

4.1 Risk Management

Principle

A *Fraud Risk Management* Framework should be defined, approved and implemented, and should be aligned with the Member Organisation's enterprise risk management process.

Control Requirements

a. The *Fraud Risk Management* Framework should be defined, approved and implemented.

b. The effectiveness of the *Fraud Risk Management* Framework should be measured and periodically evaluated using Key Performance Indicators, including at a minimum the volume and value of fraud cases.

c. The *Fraud Risk Management* Framework should be aligned with the Member Organisation's enterprise risk management process.

d. The *Fraud Risk Management* Framework should address at a minimum:
   1. *Intelligence Monitoring*.
   2. *Fraud Risk Assessment*.
   3. *Fraud Risk Appetite*.
   4. *Key Risk Indicators (KRIs)*.

e. *Fraud risk management* activities should involve, but not be limited to, the following stakeholders:
   1. Business owners and users.

2. Operational Risk.
3. *Counter-Fraud Department*.
4. Cyber and IT departments.
5. HR.
6. Digital Department.

4.1.1 Intelligence Monitoring

Principle

Member Organisations should draw on a variety of internal and external data sources to identify and monitor emerging *fraud threats*.

Control Requirements

a. The fraud *Intelligence Monitoring* process should be defined, approved, and implemented.

b. When defining the *Intelligence Monitoring* process, Member Organisations should consider the SAMA Cyber Threat Intelligence Principles.

c. The effectiveness of fraud *Intelligence Monitoring* should be subject to periodic evaluation to assess whether the sources used are comprehensive and the intelligence collated is aiding the prevention of fraud.

d. The *Intelligence Monitoring* process should include:
   1. Scanning, collation, analysis, assessment and dissemination of information on existing and emerging threats.
   2. Capturing relevant details on identified threats, such as modus operandi, actors, motivation, the origin of attacks (e.g., organised crime group, jurisdiction) and type of threats.
   3. Taking action to act on existing and emerging threats.
   4. Sharing relevant intelligence with internal and external stakeholders (e.g., Cyber, Business Operations or SAMA).

e. *Intelligence Monitoring* activities should draw on a range of information sources to develop a holistic understanding of the Member Organisation's *fraud landscape*. At a minimum, these should include:
   1. Internal Audit reports, fraud investigation output and *Fraud Scenario Analysis* covering attempted and actual fraud to identify trending fraud tactics, techniques, and procedures (TTPs).
   2. New and emerging fraud *typologies* identified by fraud detection systems, fraud investigators or the *Counter-Fraud Department*.
   3. Insights from support functions (e.g., Internal Audit, Compliance, *Cyber Security* Event and Incident Management).
   4. Reliable and relevant external sources on fraud trends both locally and globally, (e.g., government agencies, fraud forums and events, Counter-Fraud system vendors, open-source information, and subscription sources).

f. Member Organisations should, to the extent not prohibited by law or contractual terms, collaborate in sharing Counter-Fraud information including emerging fraud *typologies*, fraud threat intelligence on the groups who may be perpetrating fraud, TTPs and market trends with SAMA and other organisations in the sector.

g. Member Organisations should share log-in information for confirmed fraud cases (e.g., mobile or Device ID, IP address) through the Sectorial Anti-Fraud Committee.
h. Member Organisations should perform analysis of log-in information shared by other Member Organisations to assess the level of exposure for their own customers and record the actions completed on an analysis log sheet which may be subject to independent review.

4.1.2 Fraud Risk Assessment

Principle

Member Organisations should conduct a *Fraud Risk Assessment* to identify fraud risks to which they or their customers are subject and assess the effectiveness of controls in place to mitigate the risks.

Control Requirements

a. A Member Organisation should conduct an enterprise-wide *Fraud Risk Assessment* as part of its *Counter-Fraud Programme*.
b. The *Fraud Risk Assessment* should be based on a documented *Fraud Risk Assessment* Methodology.
c. At a minimum, the Fraud Risk Assessment Methodology should include:
    1. Identification of the *inherent risk* of fraud the Member Organisation and its customers are exposed to.
    2. An assessment of the likelihood of the *inherent risks* occurring and the impact on the Member Organisation and its customers if the *inherent risks* were to occur.
    3. Testing of the effectiveness of the controls in place to prevent, detect and respond to the *inherent risks* identified.
    4. Determination of the *residual risk* of fraud that the Member Organisation remains exposed to following testing of implemented controls.
    5. The development of action plans to address *residual risk* that is outside of risk appetite or could lead to a breach of regulations.
    6. The ongoing monitoring of action plans to validate that the risk is brought within appetite.
d. Risks identified in the *Fraud Risk Assessment* should be recorded in a formal centralised register.
e. Actions to address gaps identified in the *Fraud Risk Assessment* should be documented in a treatment plan and reviewed for adequacy and effectiveness to reduce risks.
f. The outcome of the *Fraud Risk Assessment* should be formally approved by the relevant business owner.
g. When assessing fraud risks, Member Organisations should consider:
    1. Both frauds committed by persons outside the organisation (*external fraud*) and frauds committed by or with the assistance of people employed by the organisation (*internal fraud*).

2. The output of *Intelligence Monitoring* and threat assessments.
3. Fraud incidents and loss events.
4. The modelling of potential threats to the organisation through *Fraud Scenario Analysis*.
5. Product risk – Products and services offered and how they could be used to commit fraud.
6. Customer risk – The customer base of the organisation, including, but not limited to the type of customer (e.g., Retail customer, corporate or regulated entity); the number of customers; the level of fraud awareness; and vulnerability to fraud.
7. Delivery channel risk – Channels that a customer can use to contact the Member Organisation or access their products and services, with particular consideration of the risks of remote interaction as digitalisation of products increases.
8. Transaction risk – The methods of conducting transactions, receiving funds, or transferring value.
9. Jurisdiction risk – The additional risks where products and services can be used in a foreign country.
10. *Third Party* Risk – The use of *third parties* to deliver services to the organisation or its customers.
11. *Wholesale Payment Endpoint Security* Risk – End-to-end wholesale payments risks, including communication (Member Organisation to other Member Organisation, Member Organisation to system); systems (Workstation terminal); people; and processes.

h. Member Organisations should ensure that the *Fraud Risk Assessment* fully considers cyber enabled fraud, including the interaction with the member organisation's *Cyber Security* risk management model.

i. The *Fraud Risk Assessment* should be performed at a minimum on an annual basis.

j. Member Organisations should additionally update their *Fraud Risk Assessment* for changes in the internal or external fraud risk environment. These changes include, but are not limited to:
   1. A new gap or weakness identified in the control environment.
   2. New regulatory requirements.
   3. New products and services.
   4. New channels to market and new digital platforms.
   5. New business acquisitions.
   6. Sale or disposals of parts of the Member Organisation's business.
   7. Changes in the internal environment (e.g., organisational structure).
   8. New information obtained in fraud *Intelligence Monitoring*.

4.1.3 Risk Appetite

Principle

Member Organisations should define, approve, and apply their *Fraud Risk Appetite* when designing and implementing Counter-Fraud systems and controls.

Control Requirements

a. The *Fraud Risk Appetite* of the Member Organisation should be defined to state the level of fraud risk the Member Organisation is willing to tolerate.

b. The Member Organisation *Fraud Risk Appetite* should be based on the outcome of the *Fraud Risk Assessment* and aligned to the overall risk appetite of the organisation.

c. When defining *Fraud Risk Appetite*, Member Organisations should put in place measures with associated thresholds and limits that address the impact on both:
   1. The Member Organisation (e.g., fraud losses, reputational damage); and
   2. Its customers (e.g., customer losses, number of fraud victims, inconvenience).

d. In the event that a *Fraud Risk Appetite* limit is breached with an impact on customers, a Member Organisation should escalate to *Senior Management* and initiate a crisis management process that should:
   1. Involve the CEO and other *Senior Managers* in the Member Organisation.
   2. Require meetings on at least a weekly basis until the issue is resolved and the measure returns to a level within appetite.

e. *Fraud Risk Appetite* should be reviewed on at least an annual basis and be formally endorsed by the Board.

f. *Fraud Risk Appetite* should be monitored and updated for material changes to the Member Organisation's business model.

4.1.4 Key Risk Indicators

Principle

Member Organisations should define, approve, and monitor *KRIs* to measure and evaluate position against agreed *Fraud Risk Appetite* and provide an early indication of increasing fraud risk exposure.

Control Requirements

a. The *KRIs* defined by the Member Organisation should be based on a documented methodology which should require:
   1. *KRIs* to monitor exposure against the risks identified in the *Fraud Risk Assessment*.
   2. *KRIs* to consider risks to the organisation (e.g., fraud losses, reputational impact, operational management of fraud alerts) and its customers (e.g., customer losses).
   3. *KRIs* to be approved by the CFGC or wider Risk Committee which governs the *Counter-Fraud Programme* in line with the requirements included in sub-domain 3.1.
   4. All *KRIs* to have a documented owner who is responsible for monitoring the KRI and taking early action if risk exposure exceeds *Fraud Risk Appetite*.
   5. KRIs to be periodically reported to *Senior Management* and relevant stakeholders (minimum on a quarterly basis).
   6. *KRIs* to be reviewed and updated at a minimum on an annual basis and more frequently in response to material changes to the *fraud landscape* or the Member Organisation *Fraud Risk Assessment*.

b. KRIs should be forward looking and provide an early indication of increasing fraud risk exposure rather than simply measuring fraud volumes or losses (e.g., controls rated as ineffective in control testing; failure of employees to complete mandatory fraud training; or fraud alerts not reviewed within defined service level agreements).

c. When developing *KRIs*, Member Organisations should define thresholds that allow them to determine whether the actual result of measurement is below, on, or above the targeted risk appetite position.

d. Member Organisations should ensure that metrics associated with *KRIs* are complete, accurate and generated on a timely basis.

4.2 Due Diligence

Principle

Member Organisations should define, approve and implement standards for assessing the fraud risk associated with employees, customers and third parties to prevent the establishment of relationships outside risk appetite and manage fraud risks throughout the duration of the relationship.

Control Requirements

a. *Due Diligence* standards should be defined, communicated, and implemented.

b. *Due Diligence* standards should be approved by individuals of appropriate responsibility (e.g., Employee *Due Diligence* in HR).

c. *Due Diligence* standards should consider employees, customers and *third parties*.

d. *Due Diligence* standards should be aligned to the risks identified in the *Fraud Risk Assessment*.

e. Member Organisations should review and update *Due Diligence* standards on a periodic basis and in response to material changes to the *fraud landscape*, the Member Organisation *Fraud Risk Assessment*, customer groups serviced by the Member Organisation or changes to the products or services it offers.

f. The effectiveness of the fraud *Due Diligence* standards should be measured and periodically evaluated.

g. *Due Diligence* standards should include:

   1. The *Due Diligence* checks and requirements that should be conducted to provide an informed understanding of fraud risk.
   2. When *Due Diligence* should be conducted.
   3. The role(s) responsible for conducting and approving *Due Diligence*.
   4. Red flags or warning signs which may indicate increased fraud risk and result in the requirement for escalation or further checks to be completed.
   5. Red flags or warning signs which indicate an employee, customer or *third party* is outside risk appetite and the relationship should be declined or exited.
   6. Steps to be taken to exit relationships outside risk appetite.

4.2.1 Employee Due Diligence

Principle

Member Organisations should ensure background checks are conducted on employees, including *contractors*, to reduce the exposure to *internal fraud* risks and reputational damage resulting from the actions of staff of the Member Organisation.

Control Requirements

a. Employee *Due Diligence* measures should reflect the risks of *internal fraud* impacting the Member Organisation.
b. Employee *Due Diligence* should have the objective of establishing the identity, integrity, and verifying the credentials of the employee, enabling the Member Organisation to determine whether they are suitable for the position.
c. Employee *Due Diligence* should consist of screening and background checks on the employee, including but not limited to:
    1. Confirmation of identity.
    2. Criminal background checks.
    3. Conflict of interest checks.
    4. Verification of qualifications claimed.
    5. Previous employment checks.
d. Employee *Due Diligence* should be:
    1. Conducted as part of the hiring process.
    2. Reassessed when an existing employee moves to a new role.
    3. Reperformed periodically on a risk-based approach (e.g., re-performance of screening for criminal or fraudulent behaviour to validate that employees remain suitable for the position).
e. Member Organisations should assess roles which represent a high risk of fraud and document any enhanced checks required.
f. The outcome of Employee *Due Diligence* checks should be retained in line with the Member Organisation's record management policies for personal information.

4.2.2 Customer Due Diligence

Principle

Member Organisations should establish controls to capture and validate the identity of customers to reduce the exposure to *external fraud* losses.

Control Requirements

a. When establishing a new customer relationship, Member Organisations should check and verify the identity of the customer to reasonably ensure that it is not exposed to fraud risk.
b. Customer *Due Diligence* should align with the Member Organisation's policies on Anti Money Laundering (AML) and Countering Terrorist Financing (CTF).
c. Customer *Due Diligence* should be conducted as a part of the onboarding process and at appropriate times in the ongoing relationship with the customer (e.g., addition of new credit product).

d. Customer *Due Diligence* should be enhanced with additional checks for higher risk customers or in response to a perceived increased *fraud threat* (e.g., if impersonation is suspected or there is a concern on the validity or legitimacy of documents provided to prove identity or evidence financial history).

e. Where a customer relationship is initiated on a remote basis (e.g., online), Member Organisations should assess the risk of impersonation and the set-up of mule accounts, implementing appropriate controls to mitigate the risk, including but not limited to:

   1. Ensuring a phone number or National ID/Iqama is linked to one customer application only. In the event an exception is identified (e.g., dependent family member), additional due diligence checks should be conducted to validate the authenticity of the application and monitoring use cases should be developed.
   2. Authentication of the account opening request via the National Single Sign-On portal using Biometric based authentication (e.g., facial identification from national trusted party).
   3. Verification that the ownership of the phone number is registered to the same user through a trusted party (i.e., the name of the account applicant and national ID match).
   4. Including a one-time-password mechanism (OTP) explaining that a new account is being opened as a form of verification. The OTP must be sent to the verified phone number.
   5. Notification of the completion of account opening should be sent to verified phone number that is registered for the account as well as to the phone number that is registered in the national single sign-on portal.
   6. Requiring the use of a registered National Address.
   7. Where a physical card is to be provided, this should be:
      a. Sent to the registered National Address of the customer only; or
      b. Collected from an ATM with the customer verified using biometric authentication.
   8. Following initial set up, restrictions should be placed on the account (e.g., reduced transaction value limit) until such time as the Member Organisation validates that the customer is genuine (e.g., use of biometric authentication mechanism through facial identification from national trusted party periodically, physical presence in a branch or kiosk supported by biometrics, regular pattern of account activity over a period of time).
   9. Developing comprehensive use cases to proactively identify potential mule accounts and implementing monitoring of the use cases through detection software (e.g., value of incoming funds, high transaction frequency, transaction patterns that do not fit expected behaviours, sudden increase in activity following dormancy).
   10. Measuring and periodically evaluating the effectiveness of controls to mitigate the risk of impersonation and set-up of *mule* accounts.

4.2.3 Third Party Due Diligence

Principle

Member Organisations should ensure proportionate *Due Diligence* is conducted on *third parties* to develop an understanding of fraud risk associated with business relationships and ensure *third parties* are appropriately managed to mitigate the risk.

Control Requirements

a. *Third Party Due Diligence* should consist of checks and vetting procedures on a risk-based approach to allow an assessment of the fraud risks presented by the relationship.

b. *Third Party Due Diligence* should be conducted prior to entering into a commitment for a new relationship

c. *Third Party Due Diligence* should be reviewed periodically or following a trigger which indicates increased fraud risk (e.g., concerns on the conduct of a third party or its employees; or negative media articles).

d. *Third Party Due Diligence* should be enhanced for:

   1. Higher risk *third parties* or their representatives
   2. *Third parties* providing *critical services* to the Member Organisation.

e. Enhanced *Third Party Due Diligence* checks should include additional steps to assess the fraud risks presented by the relationship (e.g., additional vetting or assessing the *third party* approach to managing the risk of fraud).

f. Where a Member Organisation outsources services to a *third party* organisation, that *third party* should comply with the Member Organisation's *Counter-Fraud Policy* or apply an equivalent approach.

4.3 Training and Awareness

Principle

A fraud awareness programme should be defined, approved, and conducted for employees, customers and *third parties* of the Member Organisation.

Control Requirements

a. The fraud awareness programme should be defined, approved, and conducted to promote awareness of fraud risks, provide education on preventing, detecting, and responding to potential fraud and create a positive *Counter-Fraud culture*.

b. The fraud awareness programme should include coverage of:

   1. Employees of the Member Organisation.
   2. Customers of the Member Organisation.
   3. *Third parties* who hold relationships with the Member Organisation.

c. The fraud awareness programme should consist of training, education and awareness materials directly linked to risks and threats identified in the *Fraud Risk Assessment*.

d. The fraud awareness programme should:

   1. Outline the nature, scale and scope of training and education to be delivered.
   2. Be tailored to the different target groups.
   3. Be delivered via multiple channels.

e. The activities of the fraud awareness programme should be conducted periodically and throughout the year.
f. Member Organisations should ensure that the programme is updated at least annually to account for changes in the fraud *threat landscape* or in response to new *fraud threats* identified in *Intelligence Monitoring*.
g. Where a new or emerging *fraud typology* may impact the Member Organisation and its customers, Member Organisations should take immediate action to make employees, customers and relevant *third parties* aware of the threat and preventive measures to be taken (where applicable).
h. Member Organisations should monitor and evaluate the effectiveness of the fraud awareness programme and implement improvements where required.

4.3.1 Employee Fraud Training and Awareness

Principle

Member Organisations should define and deliver an employee fraud training and awareness programme to enable employees to identify fraud and report it promptly.

Control Requirements

a. Counter-Fraud training should enable employees to develop a clear understanding of the Member Organisation's Counter-Fraud policies and procedures and their personal responsibilities in relation to fraud prevention and detection.
b. Training should be provided to all employees at, or shortly after, onboarding and be refreshed at regular intervals.
c. The Member Organisation's fraud training and awareness programme should be risk based, including the requirement for certain employees to be provided with specialised training depending upon the fraud risk associated with their role (e.g., managers with positions of authority, customer facing staff in branches, employees operating Counter-Fraud controls and fraud investigators).
d. Counter-Fraud training should include a knowledge check to assess whether the employee has understood the content. Employees who do not pass the knowledge check should be required to repeat the training and pass rates should be monitored, with action taken if there are repeated failures (e.g., re-training via another delivery method or removal of authority to operate a Counter-Fraud control until successful).
e. The Board of Directors and *Senior Management* at Member Organisations should be provided with fraud training tailored to the seniority of the role (e.g., fraud awareness, setting an appropriate culture and governance).
f. Formally delivered training should be augmented by ongoing employee education activity to maintain the general fraud awareness of employees (e.g., issuing reminders and circulars on potential indicators of fraud and common fraud *typologies*).
g. Member Organisations should maintain records of fraud training delivered to employees and awareness activity conducted.
h. Member Organisations should have a documented process to manage employees who are non-compliant with the training requirements for their role.

4.3.2 Customer Fraud Awareness

Principle

Member Organisations should define and conduct a customer fraud awareness programme of activity to increase customer understanding of fraud risks; help customers to recognise and resist fraud attempts; and inform them how to report fraud.

Control Requirements

a. Customer fraud awareness activity should deliver relevant and timely education to customers and promote fraud awareness.
b. The activity delivered through the customer fraud awareness programme should include, at a minimum:
    1. Information on the *fraud threats* and *scams* customers may be exposed to.
    2. Customer responsibilities about countering fraud.
    3. How customers can prevent themselves from becoming victims.
    4. How to report to the Member Organisation if the customer believes they have been a victim of fraud.
c. Customer fraud awareness activity should be tailored to the current fraud trends impacting the Member Organisation and its sector, including but not limited to the fraud *typologies* observed and the point of compromise which led to the fraud (e.g., SMS, email, social media).
d. Customer fraud awareness activity should cover the duration of the customer lifecycle (e.g., onboarding, changes to product holdings, transactions and settlements).
e. Member Organisations should deliver customer awareness materials through all communication channels offered to the customer (e.g., website, mobile app, email, post, and SMS).
f. Member Organisations should provide additional education on fraud protection to customers who may be vulnerable to or have been the victim of a *scam* (e.g., support on the phone or additional materials via email or post).

4.3.3 Third Party Fraud Awareness

Principle

Member Organisations should define and deliver a proportionate fraud awareness programme to *third parties* outlining expectations in respect of Counter-Fraud activity and prompt reporting of suspicious activity.

Control Requirements

a. *Third party* fraud awareness requirements should be documented and agreed in contractual arrangements where applicable.
b. Member Organisations should provide risk-based fraud awareness materials to *third parties* at the outset of a relationship and refresh periodically as required.
c. *Third party* fraud awareness requirements should as a minimum include:

1. The creation of a positive *Counter-Fraud culture*.
2. *Third party* roles and responsibilities regarding fraud.
3. Tailored messaging aligned to the fraud risks of the services provided by the *third party*.
4. Reporting mechanisms available to the *third party*.

4.4. Authentication

Principle

Member Organisations should define, approve, implement and maintain a standard for the authentication of customer, employee and *third party* credentials and instructions to ensure information is protected and unauthorised access or actions are prevented. This should be risk-based and utilise multi-factor authentication.

Control Requirements

a. A Member Organisation should define, approve, implement and maintain an authentication standard with input from both the *Counter-Fraud Department* and *Cyber Security* Team.

b. A Member Organisation's authentication standard should consider the risks identified in its *Fraud Risk Assessment* and *Cyber Security* Risk Assessment.

c. The authentication standard should consider both customer access to products and services, and employee and *third party* access to Member Organisation systems.

d. When defining the authentication standard, Member Organisations should take note of the following Control Requirements outlined in *The Cyber Security Framework*:
   1. 3.3.5 Identity and *access management*
   2. 3.3.13 Electronic Banking Services

e. A Member Organisation's authentication standard should cover both digital (e.g., online services and mobile app) and non-digital (e.g., phone, ATM and branch) channels.

f. Member Organisations should adopt a risk-based approach to authentication with higher risk instructions or activity subject to *multi-factor authentication* before they are acted upon.

g. *Multi-factor authentication* conducted by Member Organisations for identification or transaction verification should not solely consist of One Time Passwords (OTPs) sent via SMS. Member Organisations should implement additional factors, including but not limited to:
   1. Approval of transactions through Mobile App (e.g., sending a push notification to mobile app on a trusted device).
   2. Device characteristics (e.g., trusted/known mobile device).
   3. Geolocation (e.g., verifying location, IP address or checking mobile network).
   4. Behavioural profile (e.g., variations to usual transaction volume, value, frequency and/or currency).
   5. Biometric behavioural profile (e.g., identification of changes in the way a customer or employee uses a browser or device).

h. Where an OTP is sent via SMS, the purpose, amount and merchant name should be clearly defined in line with SAMA approved notification templates.

i. OTPs sent via SMS should be in the language selected by the customer on the account (e.g., Arabic, English).

j. Member Organisations should define high-risk instructions or activity in the authentication standard which should include, but not be limited to:
    1. Registration process for online or mobile app product access.
    2. Activating a token on a new or additional device.
    3. Adding a credit/debit card to a digital wallet on a mobile device.
    4. Reset of security credentials following failed attempts to access phone, online or remote facilities.
    5. Logging in to digital products from a previously unknown device or location.
    6. Payments to an e-wallet or digital wallet.
    7. High risk transaction, withdrawals, or transfer of funds (e.g., exceeding pre-defined limits/thresholds, transfers large relative to overall balance or remittance/international transfers).
    8. Adding or modifying beneficiaries.
    9. Change of account holder details (e.g., address or contact details).
    10. Change of language used on the account (e.g., Arabic to English).
    11. Reset of password or PIN.
    12. Issue and activation of a new debit/credit card.
    13. Reactivation of dormant accounts or blocked services.
    14. A combination of activity(s) which may be indicative of fraud or account takeover (e.g., aggregated risk score following failed log-in attempts, buying gift cards, use of new device or new geolocation).

k. Member Organisations should require a third authentication factor (e.g., a phone call to the number on the account requiring verification of secure information, a physical visit to a branch, generating a token with a temporary password linked to a device, OTP) to validate an instruction when:
    1. A user log-in attempt to mobile and online services is detected as an *anomalous session* (e.g., a device ID or location is different from previously known log-in parameters or the IP address is flagged as a risk).
    2. A transaction is instructed from a non-*trusted device* to a newly added beneficiary.
    3. An abnormal transfer rate (e.g., five transfers per hour for a retail customer) is exceeded.

l. Member Organisations should restrict activity where an *anomalous session* is identified to low level transactions until the organisation is able to authenticate the request originates from the genuine customer and can make the device *trusted*.
    1. Low level transactions should be defined by the Member Organisation in Fraud prevention standards (see 4.6).

4.5. Fraud, Financial Crime and Cyber Alignment

Principle

Member Organisations should ensure that *Cyber Security*, Counter-Fraud and *Financial Crime* Team operational capabilities are aligned to deter fraud.

Control Requirements

a. Member Organisations should define and implement a process for the alignment of the Counter-Fraud, *Cyber Security* and *Financial Crime* Team operational capabilities which should include at a minimum:
    1. Defining clear roles and responsibilities between the *Counter-Fraud Department*, *Financial Crime* and *Cyber Security* teams.
    2. Cross training between the *Counter-Fraud Department*, *Financial Crime* and *Cyber Security* Teams.
    3. The establishment of multi-disciplinary contacts between Cyber, *Financial Crime* and *Counter-Fraud* Departments to regularly share knowledge.
    4. Development of joint task forces between Counter-Fraud, *Financial Crime* and Cyber Departments to align working practice and collectively engage the wider organisation.
    5. Undertaking joint threat assessment workshops or *Fraud Scenario Analysis* with business units to collectively identify threats and share insights from *Intelligence Monitoring*.
    6. Storing relevant *threat intelligence* in a centralised repository, with access restricted to relevant stakeholders.
    7. Identification of opportunities to unify fraud and cyber prevention and detection systems and tools (e.g., provision of data on user monitoring or customer location through IP address).
    8. Alignment of Cyber, *Financial Crime* and Fraud incident response approach where incidents occur across capabilities.
    9. Co-ordination of corrective actions to disrupt the organised groups orchestrating fraud (e.g., taking down fake websites set up to capture customer details).
    10. Conducting joint retrospective lessons learnt exercises following fraud incidents that relate to data, systems, processes and controls spanning the Counter-Fraud, *Financial Crime* and Cyber capabilities.

4.6. Fraud Prevention Standards

Principle

Member Organisations should have defined, approved, implemented and maintained standards for the prevention of fraud which should be aligned to the fraud risks impacting the organisation and its customers.

Control Requirements

a. Member Organisations should define, approve, implement and maintain standards to aid the prevention of fraud addressing both *internal fraud* and *external fraud* risks impacting the organisation.

b. Member Organisations should review and update fraud prevention standards on a periodic basis and in response to material changes to the *fraud landscape* or the Member Organisation *Fraud Risk Assessment*.

c. The compliance with the fraud prevention standards should be monitored.

d. The effectiveness of the fraud prevention standards and related controls should be measured and periodically evaluated.

e. The output of the *Fraud Risk Assessment* should be used to determine where prevention activity is focused, and controls should be proportionate to the *risk appetite* of the organisation.

f. Fraud prevention standards may be manual or automated, and should include at a minimum:

   1. The controls implemented to prevent fraud (e.g., segregation of duties, approval and escalations, employee training, access restrictions, due diligence and integrity checks, notification of account changes, transaction limits, underwriting checks).
   2. Systems and technology implemented to prevent fraud (e.g., identity and access management, authentication, issuance of one-time-passwords, biometrics).
   3. Roles and responsibilities for fraud prevention (e.g., customer application review at onboarding, training design, due diligence, system testing).
   4. Rationale outlining why the prevention controls are appropriate to the risks faced by the organisation.

g. Member Organisations should define the approach to setting limits and thresholds for preventive controls (where applicable) in fraud prevention standards, considering:

   1. The outcome of the *Fraud Risk Assessment*.
   2. Fraud incidents and losses experienced.
   3. *Fraud Risk Appetite*.

4.6.1 Internal Fraud

Principle

Member Organisation fraud prevention standards should include controls designed to prevent *internal fraud*.

Control Requirements

a. A Member Organisation should include in its fraud prevention standards, controls to mitigate the risk of *internal fraud* occurring, including but not limited to:

   1. Requiring employees to adhere to a *Code of Conduct*.
   2. Requiring all employees to take block leave of a minimum continuous period of 10 working days each year.
   3. Segregation of duties in payment and fulfilment processes supported by documented authorisation matrices.
   4. Dual controls or secondary checking of control operation, with an additional review or approval process for transactions above thresholds defined by the Member Organisation (e.g., value of transaction or payments to a new supplier) or higher risk transactions (e.g., access to dormant accounts).

5. Restricting access to secret customer details for all employees (e.g., online credentials, OTP messages).
6. Restricting access to confidential customer account data (e.g., account balance, loan amount) where visibility is not required in the job role (e.g., IT employees). Where access is required, activity should be logged and securely stored (see control requirement 5.3.b).
7. Requirements for appropriate handling of confidential data.
8. Controls over access to cheques and cash.
9. Controls to safeguard the physical security of assets (e.g., requiring staff identification at all times, securing and tracking equipment and restricting access to sensitive assets).

b. Member Organisations should take note of the Identity and *Access Management* Control Requirements relating to user *access management* and privileged *access management* outlined in *The Cyber Security Framework*.

c. Member Organisations should ensure that individuals responsible for operating *internal fraud* controls are sufficiently independent from the individuals they are monitoring.

d. Member Organisations should put in place appropriate processes and controls to deter and avoid conflicts of interest and related party transactions for their directors, managers, employees, external businesses, and *contractors*, including but not limited to:
   1. Creating a policy that clearly outlines prohibited behaviour.
   2. Limiting the flow of information between internal departments and employees through information barriers.
   3. Providing guidance, instructions and examples on avoiding conflicts of interest.
   4. Requiring immediate disclosure of any conflicts or potential conflicts.

4.6.2 External Fraud

Principle

Member Organisation fraud prevention standards should include controls designed to prevent *external fraud*.

Control Requirements

a. A Member Organisation should include in its fraud prevention standards, controls to mitigate the risk of *external fraud* occurring, including but not limited to:
   1. Hotline available 24 hours to report suspected fraud and take immediate action to respond to the fraud (e.g., blocking account access or cards).
   2. The provision of an *emergency stop* self-service capability for customers to immediately freeze their account and block further transactions if they suspect their account has been compromised.
   3. Customer identity and *access management* controls for online/mobile accounts and digital products.
   4. Use of *blacklists* to screen and block transactions, card provisioning or access from identified high risk:
      a. Accounts

    b. IP addresses
    c. Email addresses
    d. Compromised devices or those that have previously been used for fraud (e.g., mobile phone app registered to an account which has been used to conduct fraud).
5. The capability to swiftly block transactions from customer accounts/cards, with defined safeguards in place to release the block.
6. Requiring users of online and mobile services to consent to the activation of GPS during an active session to allow the organisation to monitor location.
7. The capability for mobile apps to detect use on devices which have subject to jailbreaking or rooting, and subsequently block the use of the app or restrict access to sensitive data or features.
8. Prohibiting the use of VPN services when accessing online or mobile services.
9. Device registration which allows users to register *trusted devices* for *access management*.
10. A restriction on concurrent log-ins to mobile app or a limitation on the number of devices which a mobile app can be installed and accessed.
11. The identification of *mule accounts* (e.g., accounts set-up to receive fraudulently obtained funds and launder the proceeds of crime).
12. User behaviour profiles which allow rules to be implemented to prevent access to customer accounts if unusual behaviour is identified.
13. Monitoring of product inactivity and dormancy, particularly where products are reactivated.
14. Notification sent to the customer when changes are made to *static data* to previous and new details.
15. Online, mobile and phone payments:
    a. Sending an OTP to verify all payments instructed (new and existing beneficiaries), including transactions through remittance accounts.
    b. Notification to the customer of new payees added (e.g., SMS, call back).
    c. Setting a default limit for single and daily transactions which should be periodically reviewed and updated where required (e.g., review of customer profiles and behaviours, and actual fraud cases/customer losses).
    d. Notify the customer if the default transaction limit is increased (e.g., if the customer account type is upgraded).
    e. The option for customers to reduce the default limit for a single transaction.
    f. The option for customers to reduce the default limit for daily transactions.
    g. An immediate block on further transactions if a transaction limit is reached either through individual or recurring payments whether to one or multiple beneficiaries.
    h. Additional verification checks to authenticate:
        i. Unusual transactions (e.g., transactions after a period of account dormancy, changes to customer behaviours).
        ii. Unusual patterns of transactions (e.g., multiple payments to the same beneficiary in a short period).

        iii. Transactions exceeding a defined value threshold.
        iv. Requests to increase the single or daily transaction limit.
        v. Initial transactions after registration for online banking or mobile services, or registration of a new device.
    i. Additional verification checks should include but not be limited to, one or more of the following:
        i. Automated call-backs.
        ii. Manual call-backs.
        iii. SMS to registered mobile number.
        iv. Authentication via biometrics on registered mobile device.

16. Credit and debit cards:
    a. Adherence to all card scheme rules (e.g., mada business rules, Visa CVV2 code, Mastercard CVC2 code).
    b. Use of one-time passwords (OTPs) to approve online transactions.
    c. For high risk transactions, the use of extra authentication measures in addition to OTPs or mobile app approval (e.g., automated call-back to the phone number on the account).
    d. Address/Postal code verification for online card payments.
    e. New cards issued to require activation before use.
17. Validation controls to ensure the authenticity of cheques and similar instruments.
18. Periodic inspection of ATMs for evidence of suspicious activity or devices that could compromise card security.
19. Removal of clickable links in all emails and SMS sent to customers.

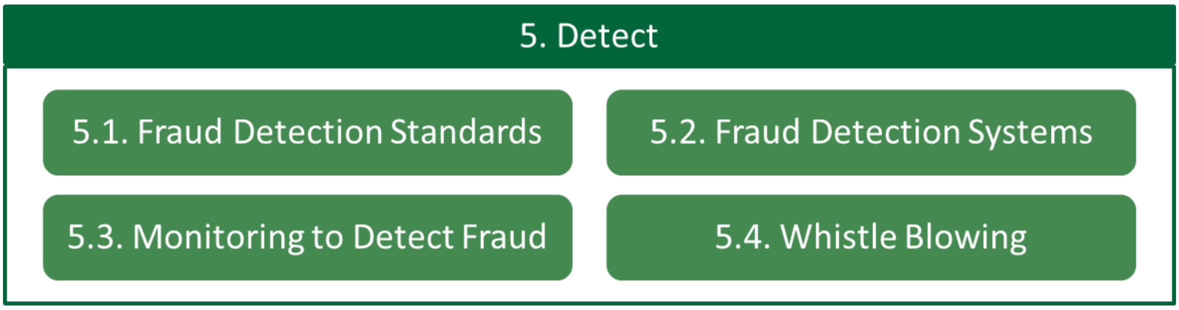
b. Member Organisations should additionally implement the following preventive controls on a risk-based approach:
    1. A delay to activation when a customer requests an increase in online/mobile transaction limits.
    2. Robotic prevention mechanisms prior to the instruction of a payment to mitigate the risk of automated bot activity.
    3. Functionality for customers to request instant notification of all account and card transactions to their registered mobile device.
    4. *Geofencing* when transactions occur in a location outside the customers home area (e.g., using mobile device geolocation data to require verification if a user attempts to access products and services while in a foreign country which is not in line with user behaviour profile).
    5. Procedures for holding suspicious transfers to countries classed as high-risk in the organisation’s jurisdiction risk model.
    6. A delay to payments requested for new payees added via online/mobile services until further verification is completed.
    7. Introducing a delay before a new soft token can be activated on a mobile device.
    8. Notifying the customer of the registration of a new device and identifying critical services (e.g., card provisioning, addition of new payees) which should be disabled for a period following the new device registration.

c. Member Organisations providing lending and credit products should include in fraud prevention standards, controls to mitigate the risk of *external fraud* occurring, including but not limited to:

   1. Review of applications/proposals to check for potential application fraud (e.g., manipulation of details or misrepresentation of the applicant’s financial position).
   2. Checks for fraudulent or counterfeit documents provided for identification or as security on lending.
   3. Panel management controls for agents, intermediaries, valuers and other third parties.

5. Detect

It is vital for the security and protection of customers to quickly identify actual or attempted fraud where preventative controls are insufficient or have failed. Fraud detection systems and controls are risk-based measures to identify fraud by looking for indicators in customer behaviours, transactional and non-transactional information. Effective detection of fraud enables proportionate and timely action to minimise organisational losses and customer impact. Detective controls can be manual, but typically given the volume of activity in financial institutions and digital nature of products and services, rely on technology to perform automated monitoring.



5. Detect

5.1. Fraud Detection Standards

5.2. Fraud Detection Systems

5.3. Monitoring to Detect Fraud

5.4. Whistle Blowing

Figure 6 – Detect Domain

5.1. Fraud Detection Standards

Principle

Member Organisations should have defined, approved, implemented and maintained fraud detection standards which should be aligned to the fraud risks impacting the organisation and its customers.

Control Requirements

a. Member Organisations should define, approve, implement and maintain fraud detection standards addressing both *internal fraud* and *external fraud* risks impacting the organisation.

b. Member Organisations should review and update fraud detection standards on a periodic basis and in response to material changes to the *fraud landscape* or the Member Organisation *Fraud Risk Assessment*.

c. The compliance with fraud detection standards should be monitored.

d. The effectiveness of fraud detection standards and related controls should be measured and periodically evaluated.

e. The output of the *Fraud Risk Assessment* should be used to determine where detection activity is focused, and controls should be proportionate to the *risk appetite* of the organisation.

f. Where the *inherent risk* of fraud is assessed as higher, the fraud detection standards should require additional detection controls (e.g., real time monitoring, additional data sources or *Machine Learning* models) or more stringent detection threshold criteria (e.g., lower monetary limits before an alert is raised).

g. Fraud detection standards should include at a minimum:
   1. Data sources used to inform detection of suspicious activity and fraud (e.g., core customer records, transactional/payment systems, identity and *access management*, external databases).
   2. The controls implemented to detect suspected fraudulent activity (e.g., escalation of high-risk events and transactions, secondary checking, reconciliations, exception reporting, internal training).
   3. The controls implemented to detect suspected fraudulent activity relating to W*holesale Payment Endpoint Security* (e.g., monitoring of payments behaviour and out-of-band reports, the creation of a counterparty white-list, anomalous payment tracking, blocking of payments in real-time).
   4. Systems and technology implemented to detect potential fraud (e.g., fraud detection software, alerts on high-value events or transactions, access monitoring, link analysis).
   5. Roles and responsibilities for fraud detection (e.g., system calibration, reviewing manual fraud referrals, alert triaging and management, escalation point for potentially significant incidents, supervision and oversight).
   6. Rationale outlining why the detection systems and controls are appropriate to the risks faced by the organisation.

h. Member Organisations should consider the following areas of activity when documenting the people, process, and technology requirements for fraud detection:
   1. Employee activity data (e.g., system access, invoices and payments, approvals).
   2. Customer account activity (e.g., transactions, payments, settlement).
   3. Customer account access and management (e.g., log-in geolocation, device usage, changes to *static data*).
   4. *Third party* activity data (e.g., access to and use of Member Organisation systems or data, instructions on behalf of customers, referrals from agents).

i. Where a Member Organisation determines a manual control is required (e.g., due to the scale of the Member Organisation, lack of systems or analytics, or coverage of products and channels), the nature of the fraud risk should be reviewed to assess the number of employees and skills required to provide adequate manual coverage.

j. Member Organisations should have adequate resources in place to manage the outputs from manual and automated fraud detection (e.g., sufficient employees to work alerts, appropriate skills and training for employees to complete investigations, workflow system to allocate alerts).

5.2. Fraud Detection Systems

Principle

Member Organisations should implement and maintain fraud detection systems to identify anomalies in transactional and non-transactional data, and customer or employee behaviour that may be indicators of fraud.

Control Requirements

a. Member Organisations should implement and maintain fraud detection systems to monitor customer products and services, and internal systems for transactions or behaviours that may be indicative of fraud.

b. Fraud detection systems should operate 24/7 with appropriate resources in place to manage outputs on a timely basis.

c. Member Organisations should develop holistic and current sources of data to be used to inform detection of suspicious activity and fraud, including at a minimum:
   1. Customer products and services held across all lines of business.
   2. All contact channels (e.g., online, mobile, phone).
   3. External information (e.g., credit reference data, *blacklists*, vendor provided data sets).
   4. The insights gathered from *Intelligence Monitoring* (see sub-section 4.1.1).
   5. Transactional or settlement data (e.g., payment values into or out of accounts, payment recipients added, authority for payment instruction, transfer from custodian of funds).
   6. Non-transactional data (e.g., employee behaviour, online access, device usage, geo-location, changes to s*tatic data*).

d. Member Organisations should implement controls (e.g., data governance, de-duplication, data quality alerts, regular audit, integration testing, regression testing for change management) to ensure that the underlying data is:
   1. Timely – Supplied to the detection system at an appropriate frequency based on the rate of change and urgency of information (e.g., payment data should be real-time to allow intervention before funds are transferred, while new products sold may be updated daily, and external information refreshed when lists change).
   2. Complete – Includes all required data from all relevant systems identified in the Counter-Fraud detection standards (e.g., data mapping from source system to the detection system should be validated).
   3. Accurate – Of sufficient quality to enable effective monitoring (e.g., up to date, tested to ensure data quality).

e. Member Organisations should ensure fraud detection system capability includes at a minimum:
   1. Analysis of structured data (data in a standardised, well-structured format).
   2. Monitoring of customer and internal accounts.
   3. Baselining of user behaviour patterns into profiles which allow deviations from normal activity to be identified (e.g., expected frequency or value of transactions).
   4. Definition of a library of *rules* based on known fraud *typologies* to identify activity which could be indicative of fraud (e.g., employee access patterns, unknown or remote customer location, increased frequency of transactions, new transaction type, high value amount, recurring transactions whether to one beneficiary or multiple beneficiaries, single source of transfer to many accounts).
   5. Segmentation of customer groups to enable tailoring of *rules* (e.g., modifying *rules* and thresholds based on different expected behaviours of a high-net-worth Private

Banking customer vs. a standard Retail customer or a new account opened online vs. an established relationship managed customer).

6. Applying a weighting to *rules* based on the assessed level of fraud risk and assigning risk scoring to identify activity that may be indicative of fraud.
7. The aggregation of risk scores to assess patterns of transactional and non-transactional activity across multiple channels that when combined may be indicators of fraud.
8. Linking outputs (e.g., alerts and cases for further investigation) to a *Case Management System*.

f. Member Organisations should use the output of *Intelligence Monitoring* and information from across the organisation in data analytics to deeply analyse current status, predict future fraud threats and take proactive action to prevent fraud. Analytics should use multiple data sources, including but not limited to historical and current trends, customer data, transactions and non-transactional activity.

g. Where a higher risk of fraud is identified in the *Fraud Risk Assessment* or higher incidences of fraud occur, Member Organisations should additionally implement system capability of:

1. Big data mining to facilitate advanced analytics over large quantities of structured and unstructured data, with associated orchestration to create a centralised data repository (e.g., using data refinement and comparison algorithms to perform queries on very large volumes of data, and storage in a data lake).
2. Analytical tools and capabilities to enhance *rules*-based monitoring (e.g., *trend analysis*, *keyword analysis*, *predictive analytics,* and *anomaly detection*).
3. Overlaying *Artificial Intelligence* and *Machine Learning* algorithms (e.g., decision trees, random forests, neural networks) to:
    a. Enhance system decision making capability.
    b. Predict the likelihood of fraud.
    c. Learn from historical patterns of fraudulent and legitimate behaviour.
4. Network Visualisation/Link analytics or *Entity Resolution* to reveal hidden or previously unknown connections and identify networks across different data sources (e.g., identify connections from devices or IP addresses known to have been used for fraudulent purposes and link with other data points to create a threat score associated with a network, by looking at location, payment cards used, beneficiaries etc.).
5. Analysis of additional unstructured external data (e.g., scanned customer documents) to widen data sources.

h. Where a deviation from the baselined user behaviour patterns is identified, Member Organisations should either:

1. Require further authentication of the user or their instructions.
2. Generate an alert for further investigation to determine whether fraud has occurred.

i. To ensure the effectiveness and optimisation of fraud detection systems, Member Organisations should:

1. Calibrate and test detection scenarios to validate they are working as designed and enabling monitoring in accordance with the organisations risk appetite (e.g., *rule* logic review, threshold testing, *precision and recall testing*).
2. Implement feedback loops to monitor and enhance the performance of systems and effectiveness of scenarios and parameters by reviewing false positives, false negatives and alerts which identified fraud.
3. Periodically review scenarios and parameters to ensure they remain appropriate in view of the insights gathered in *Intelligence Monitoring* and/or the outcome of the *Fraud Risk Assessment*.
4. Periodically test the effectiveness of systems, through ongoing tuning and calibration measures such as data mapping and input validation, *model validation*, scenario effectiveness testing and reporting.
5. Update user behaviour patterns and *rules* to account for the latest threats and fraud *typologies*.
6. Retain a documented record of changes made to configuration or *rules* and the rationale for the decision.
7. Monitor for unauthorised changes to the system (e.g., *rule* tampering or disabling of monitoring).

j. The fraud detection systems should have the capability to monitor and report metrics and *Management Information* in respect of:
    1. Data integrity.
    2. *Rule* and scenario effectiveness (e.g., false positive rate).
    3. Operational performance.

5.3. Monitoring to Detect Fraud

Principle

Member Organisations should design and implement controls to monitor activities and behaviour in order to detect potential indicators of *external fraud* and *internal fraud*.

Control Requirements

a. Member Organisations should design and implement controls to monitor customer products and services for behaviours that may be indicative of external fraud. At a minimum these should address the risk presented by:
    1. First party fraud – Where a customer of the Member Organisation misrepresents their identity or gives false information to commit fraud using their own account, loan application or other product.
    2. Second party fraud – Where a customer or individual knowingly provides their personal information or allows their identity to be used to commit fraud.
    3. Third party fraud – Where a non-customer of the Member Organisation obtains a customer’s details without their consent or knowledge, then uses the information to commit fraud.

b. Member Organisations should design and implement controls to monitor employees in roles which have been identified in the *Fraud Risk Assessment* as presenting a risk of *internal fraud*, including but not limited to:
   1. Audit trail of employee access to the Member Organisation's core systems.
   2. Systematic log of staff activity for all customer and financial accounting systems and databases (e.g., recording an audit trail of an employee making changes to a customer address, adding a payee, instructing a payment, authorising a withdrawal).
   3. Monitoring for unusual behaviours or activity (e.g., transactions outside working hours, process exceptions or overrides completed without appropriate approvals).
   4. Reconciliation and settlement of finance systems and organisation internal bank accounts.
   5. Enhanced oversight of payments to Member Organisation employee's accounts.
   6. Monitoring and appropriate approval of corporate card use and expense claims.
   7. Monitoring of employee complaints and anonymous reporting lines.

5.4. Whistle Blowing

Principle

Member Organisations should define, approve, implement and maintain a process to enable concerned employees and *third parties* to report potential fraud *violations* without the fear of negative consequences or repercussions.

Control Requirements

a. Member Organisations should define, approve, implement and maintain a whistle blowing process across multiple channels for employees and *third parties* to report potential fraud *violations*.

b. The process should comply with SAMA's *Whistle Blowing Policy for Financial Institutions (Whistle Blowing Policy*).

c. Member Organisations should take no action against whistle blowers for any disclosures of potential fraud *violations* reported in good faith.

6. Respond

A timely and effective response to incidents of actual or suspected fraud is key to minimising losses and maximising the opportunity for recovery. Where fraud is suspected or detected, a robust *Fraud Response Plan* including clear procedures is required to manage the response, enabling effective investigation; a prompt, fair resolution; and corrective action where required. Following resolution, it is key to evaluate the root cause of an incident and assess effectiveness of control frameworks to avoid recurrence.

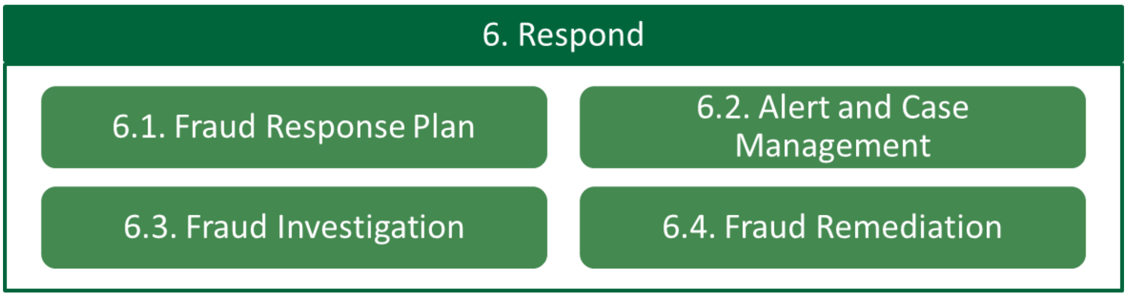


Figure 7 – Respond Domain

6.1. Fraud Response Plan

Principle

Member Organisations should define, approve, implement and maintain a *Fraud Response Plan* to outline the organisational response to an actual or suspected fraud incident.

Control Requirements

a. The *Fraud Response Plan* should be defined, approved, implemented, maintained and where appropriate aligned with the enterprise incident management process.

b. The compliance with the *Fraud Response Plan* should be monitored.

c. The effectiveness of the *Fraud Response Plan* and related controls should be measured and periodically evaluated.

d. The *Fraud Response Plan* should require prompt and competent assessment, investigation, and resolution of all suspected or identified fraud.

e. The *Fraud Response Plan* should include at a minimum:

   1. The methods through which the Member Organisation is alerted to suspected or identified fraud, including reporting channels available to customers, employees and *third parties*.
   2. Roles and responsibilities for individuals and teams required to respond to a potential fraud.
   3. Decision making authority and referral procedures for escalations within and outside the Member Organisation (e.g., referral to specialists for complex cases, *Senior Management* for potentially material frauds, external counsel if there are legal concerns).
   4. *Service Level Agreements (SLAs)* for response to initial fraud reports.

5. Procedures to quickly respond to potential fraud cases identified by the Member Organisation, informed by the customer or notified by other organisations. This should include precautionary measures to freeze funds received until the integrity of the source is verified if it is suspected that inbound transactions are the result of fraud.
6. The actions the Member Organisation will take when fraud is suspected or has been identified, including but not limited to:
    a. Coordinating appropriate resources to manage alert and case volumes.
    b. Recording and performing an initial assessment of all alerts or formally submitted reports of fraud.
    c. Where an alert or referral is assessed as not requiring further investigation, recording a rationale explaining the decision.
    d. Investigating all instances where it is suspected fraud may have been committed or has been identified.
    e. Keeping a comprehensive record of all evidence and investigations of potential and actual fraud for a period defined in the record retention schedule of the Member Organisation and in compliance with Article 12 of the Anti-Money Laundering Law.
7. The process to be followed in the event a potential fraud incident is detected outside of the normal working hours of the Member Organisation.
8. The requirement to initiate an immediate response when a potential *Wholesale Payment Endpoint Security* fraud is identified.
9. Where an actual or potential fraud relates to services offered to a customer or a payment to/from a Member Organisation or a customer, the *Fraud Response Plan* should require Member Organisations to:
    a. Identify if a potentially fraudulent transaction has been completed or is in the process of being completed.
    b. If a transaction has not been completed: Take immediate action to block or hold the transaction and proactively coordinate with any corresponding Member Organisations to take the required actions taking into consideration the role of Sharing Room – Operational Centre.
    c. Proactively respond to requests relating to suspected fraudulent transactions when receiving a notification from another Member Organisation based on agreed protocols for the Sharing Room – Operational Centre.
    d. Block or freeze the product (or any associated services such as compromised credit or debit cards) to prevent further transactions until the investigation is complete and where necessary security credentials are reset or a new card is issued.
    e. Block any further transactions to or from any IBANs outside the Member Organisation which were used to perpetrate the fraud and share the IBAN with the external organisation to freeze the account.
    f. Cooperate with other organisations if a request for freezing a product is received and there are justifications for suspicion.

g. If a transaction has been completed and an investigation confirms a transaction is fraudulent: Reverse the transaction or seek return of funds where possible.
h. Contact the customer or third party to communicate actions taken and next steps.
i. Verify the identity of the customer before re-activating services after an account has been frozen due to exposure to fraud.

6.2. Alert and Case Management

Principle

Member Organisations should implement and maintain a *Case Management System* to manage the response to fraud. This should facilitate the recording, monitoring and storage of data on the assessment, investigation, and resolution of suspected and identified fraud.

Control Requirements

a. Member Organisations should implement and maintain a *Case Management System* to manage the response to fraud and act as a database for fraud case data.
b. The *Case Management System* should be used to record and monitor suspected fraud alerts, internal and external reports, and case investigations from initial assessment to resolution.
c. The *Case Management System* should have the capability to:
    1. Restrict user access to authorised individuals and roles.
    2. Create a workflow aligned to the operating model of the Member Organisation.
    3. Be configurable to adapt to changes in the Member Organisation operating model or *Fraud Response Plan*.
    4. Allocate cases to owners.
    5. Categorise suspicions of fraud to inform reporting and *trend analysis*.
    6. Track a case from initial alert or report to resolution.
    7. Record investigative steps followed.
    8. Act as a repository for all information required to investigate and resolve the fraud case (e.g., related party information, case notes, documentary evidence, customer communication, rationale for decision).
    9. Capture an outcome at resolution of the case, including any losses and corrective actions.
    10. Maintain records in line with the Member Organisation’s record retention schedule.
d. The *Case Management System* should require the capture and allow the extract of *Management Information* for reporting on fraud cases, including but not limited to:
    1. Alert unique identifier (where applicable).
    2. Fraud transaction unique identifier.
    3. Date of alert or initial notification.
    4. Date and time of fraudulent transactions.
    5. Customer name and account number.

6. Case status.
7. Origin of the incident (e.g., website, social media account or phone number used by the fraudster).
8. Channel used for fraudulent transactions.
9. Related parties.
10. Information on the fraudster (e.g., IP address, Device ID, Geolocation).
11. Outcome of the investigation.
12. Corrective actions.
13. Value of the fraud.
14. Losses (business and non-business).
15. The methods used to conduct the fraud/fraud typology (e.g., how the fraud was committed, where the funds were transferred if lost).

6.3. Fraud Investigation

Principle

Member Organisations should define, approve, implement and maintain a fraud investigation standard to direct a consistent approach to fraud investigation.

Control Requirements

a. Member Organisations should define, approve, implement and maintain a fraud investigation standard.
b. The compliance with the fraud investigation standard should be monitored.
c. The effectiveness of the Fraud Investigation standard and related controls should be measured and periodically evaluated.
d. The fraud investigation standard should direct a consistent approach to fraud investigation, including but not limited to:
    1. Allocation of the case to an individual or team with the required skills and experience.
    2. Assessing the time sensitivity of the fraud or potential fraud (e.g., will losses increase if the case is not resolved, has a customer been left without access to funds).
    3. Assessing the materiality of the fraud or potential fraud (e.g., number of customers impacted, potential losses, systemic threat).
    4. Gathering and analysing information to review the suspicion of fraud (e.g., transaction information, IP addresses used, phone recordings, CCTV footage).
    5. Collaborating with relevant internal subject matter experts and stakeholders (e.g., Legal, Cyber, HR, *Financial Crime*) and where relevant forming a multi-disciplinary investigation team.
    6. Assessing the skills required to conduct the investigation in more complex cases (e.g., forensic accounting, data analysis).
    7. Contacting the customer or *third parties* to obtain further information.
    8. Liaising with other Member Organisations to share information.
    9. Documenting the investigative steps taken.

10. Managing and retaining information gathered.
11. Evaluating whether fraud has occurred and resolving or closing the investigation.
12. Recording an outcome of the investigation.
13. Producing a case report and internally reporting the outcome of the investigation where required.
14. Taking corrective action at the conclusion of the investigation.
15. Determining external notifications required (e.g., liaising with law enforcement, notifying credit reference agencies, reporting to SAMA, reporting to the General Directorate of Financial Intelligence (FIU) if the Member Organisation has any suspicion that rises to the level stated in article 15 of AML Law and article 17 of CTF law).
16. Identifying the root cause of fraud incidents and *near misses*.
17. Extracting lessons learnt and providing feedback to:
    a. The *Counter-Fraud Department*.
    b. Team responsible for developing and maintaining Counter-Fraud systems.
    c. Business owners of standards, processes, and controls where a vulnerability is identified.
    d. *Intelligence Monitoring.*

e. The fraud investigation standard should require corrective action to be taken where relevant at the resolution of a fraud investigation.

6.4. Fraud Remediation

Principle

Member Organisations should define, approve, implement and maintain a process to identify the root cause of a fraud incident, determine any lessons learnt and take corrective actions to prevent a recurrence.

Control Requirements

a. Member Organisations should define, approve, implement and maintain a process to identify the root cause of a fraud incident at the conclusion of an investigation. At a minimum the process should include:
    1. Understanding the point of compromise (e.g., the channel which was used to perpetrate the fraud or take control of an account).
    2. Determining whether other parties could have been involved in the fraud (e.g., additional employees through collusion or persons known to the customer).
    3. Reviewing whether a preventive control has failed or been bypassed by an employee.
    4. Evaluating whether the fraud was identified proactively by a detective control or relied on reactive customer notification.

b. Following determination of the root cause, Member Organisations should define, approve and implement a process to determine lessons learnt and inform corrective actions to prevent a recurrence. At a minimum the process should include:

1. Collating data which may support the analysis of patterns in fraud cases, including but not limited to IP addresses used, beneficiary accounts, device IDs involved.
2. Assessing whether there is a gap in the current control framework.
3. Determining whether other departments of the Member Organisation have the same vulnerability.
4. Evaluating whether the issue could impact other Member Organisations and sharing relevant information that may prevent a recurrence (e.g., fake websites impersonating government entities or social media accounts).
5. Documenting corrective actions to address the root cause and prevent a recurrence.

c. Member Organisations should take corrective actions to remediate the root cause and/or the impact of a fraud incident, which may include but are not limited to:
   1. Implementing a new control or enhancing an existing control.
   2. Providing training or communicating new awareness materials to improve employee, customer or *third party* awareness.
   3. Putting a fraud victim back into the position they were in prior to the incident (e.g., reimbursing stolen funds, chargebacks, refunding a *scam* payment, repaying a *third party*).
   4. Providing support to a victim of fraud (e.g., informing of next steps, providing a new card, providing education).
   5. Attempting to recover funds or assets.
   6. Exiting a customer or *third party* relationship if they are found to be the perpetrator of a fraud.
   7. Internal disciplinary action where *internal fraud* is identified.
   8. Liaising with law enforcement.

d. The acceptance and implementation of corrective actions should be tracked by the Counter-Fraud Department with escalation to the CFGC where actions are rejected by the business or remedial action is delayed.

Appendices

Appendix A – Defined Terms

The following are considered defined terms for the purpose of this Framework.

Defined Term	Definition
Access Management	The process of granting authorised users the right to use a service, while preventing access to non-authorised users.
Anomalous Session	Log-in sessions to mobile or online services that have different log-in parameters to those previously used by the customer, e.g., Device ID or location; or when the IP address is flagged as a risk.
Anomaly Detection	Finding patterns in data that depart significantly from the expected behaviour. Fraud anomaly detection can be implemented as an intelligence tool using unsupervised Machine Learning algorithms.
Artificial Intelligence	The use of computer systems to perform tasks typically requiring human knowledge and logical capabilities, often in problem solving scenarios.
Black Box System	A complex system where the internal rules and mechanisms are not visible to or understood by the system owner.
Blacklist	A list of untrustworthy or high risk individuals or entities that should be excluded and avoided. Also known as block-list.
Case Management System	A system used to manage alerts and fraud incidents from an initial report, through investigation, resolution and remediation where required.
Code of Conduct	A defined set of expectations which outline principles, values, and behaviours that an organisation considers important to its operations and success.
Contractor	An individual or organisation under contract for the provision of services to an organisation.
Counter-Fraud Culture	The shared values, beliefs, knowledge, attitudes and understanding about fraud risk within an organisation. In a strong Counter-Fraud culture people proactively identify, discuss, and take responsibility for fraud risks.
Counter-Fraud Governance	A set of responsibilities and practices exercised by the Board, Executive and Senior Management with the goal of providing strategic direction for countering fraud, ensuring that Counter-Fraud objectives are achieved,

	ascertaining that fraud risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
Counter-Fraud Governance Committee (CFGC)	An established group of individuals tasked with providing oversight and direction, and ensuring that the organisation’s combined Counter-Fraud capabilities are functioning appropriately and efficiently.
Counter-Fraud Maturity	The extent to which an organisation’s resources are effectively implemented for the purpose of countering fraud in comparison to global accepted standards and best practice.
Counter-Fraud Policy	A set of criteria for the provision of Counter-Fraud activities. It sets the commitment and objectives for Counter-Fraud and documents responsibilities.
Counter-Fraud Programme	A collection of policies, processes, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that are used to protect the Member Organisation and its customers against internal and external fraud threats.
Counter-Fraud Strategy	A high-level plan, consisting of projects and initiatives, to mitigate fraud risks while complying with legal, statutory, contractual, and internally prescribed requirements.
Counter-Fraud Department	A dedicated department or team established for the purpose of managing the implementation of the organisation’s Counter-Fraud objectives.
Critical services	Services provided by a third party where a failure or disruption in the provision of services could leave the Member Organisation unable to serve its customers or meet its regulatory obligations.
Cyber Security	Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the Member Organisation's information assets against internal and external threats.
Due Diligence	The investigation of an employee, customer or third party to confirm facts and that it is as presented.
Emergency Stop	A self-service capability for customers to immediately freeze their account and block further transactions if they suspect their account has been compromised
Employee	Employees encompass members of the Board of Directors and its committees, Executives, permanent and contract employees, consultants, and employees working through a third party

Entity Resolution	A process to identify data records in a single data source or across multiple data sources that refer to the same real-world entity and to link the records together.
External Fraud	A fraudulent event conducted by any persons on the 'outside' of the organisation i.e., not employed by the organisation.
Financial Crime	Criminal activities to provide economic benefit including money laundering; terrorist financing; bribery and corruption; and market abuse and insider dealing.
Fraud	Any act that aims to obtain an unlawful benefit or cause loss to another party. This can be caused by exploiting technical or documentary means, relationships or social means, using functional powers, or deliberately neglecting or exploiting weaknesses in systems or standards, directly or indirectly.
Fraud case	An individual occurrence of fraud recognised by an organisation.
Fraud Landscape/Threat Landscape	Fraud threats, trends, and developments in the political, economic, social, technological, or legal environment.
Fraud Response Plan	A plan which details the actions to be undertaken when a fraud is suspected or has been detected. This will include reporting protocols, team responsibilities and information logging.
Fraud Risk Appetite	The level of fraud risk that an organisation is willing to accept or tolerate in pursuit of its objectives.
Fraud Risk Assessment	A process aimed at addressing the organisation's vulnerability to fraud. This will include identification of fraud risks, assessment of the likelihood that fraud risks will occur and the resulting impact, determination of the appropriate response, and review of the control framework.
Fraud Risk Management	The ongoing process of identifying, analysing, monitoring, and responding to fraud risks to which the organisation and its customers are exposed.
Fraud Scenario Analysis	The testing of devised fraud scenarios for the purpose of assessing the current capability of fraud systems within the organisation.
Fraud Threat	Any circumstance or event with the potential to result in a fraud event occurring.
Fraud Typology	A categorisation of a fraud event based on its methodology and common themes with other fraud events.
Geofencing	Restricting access to online or mobile services based upon the user's geographical location.

Incident	A fraud case or series of associated cases.
Inherent Risk	The fraud risks posed to the organisation's business operations or its customers if there were no controls present.
Intelligence Monitoring	The process of continually reviewing and gathering intelligence on new and emerging fraud threats and typologies from a comprehensive range of sources.
Internal Fraud	Fraud committed by or with the assistance of people employed by the organisation.
Key Risk Indicators (KRIs)	A measure used to indicate the probability an activity or organisation will exceed its defined risk appetite. KRIs are used by organisations to provide an early signal of increasing risk exposures in various areas of the enterprise.
Keyword Analysis	Codifying rules to match key words on a look-up table to those within key fields of a fraud case record. Complexity can be added to rules such as requiring the words to be in a particular order or high-risk terms that have often indicated fraud.
Machine Learning	The use of computer systems that have the capability to learn and adapt without explicit instruction through the use of algorithms or models to analyse and build on patterns and trends in data.
Management Information	Information collated and then presented, often in the form of a report or statement, to management or decision makers for the purpose of identifying trends, solving issues and/or forecasting the future.
Member Organisation	All financial institutions or financial services providers regulated by SAMA.
Model Validation	Analysis to assess whether the outputs of a system are performing as expected.
Mule accounts	Accounts set-up (often via remote or online channels) to receive fraudulently obtained funds and launder the proceeds of crime.
Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include something you know (e.g., password/PIN), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric).
Near Misses	Potential fraud incidents that are detected and remediated prior to the fraud incident resulting in a monetary loss.
Policy Breach	The failure to comply with or disregard of policy requirements.

Precision and Recall Testing	Metrics to evaluate the effectiveness of models. Precision: The ability of a classification model to identify only the relevant data points. Recall: The ability of a model to find all the relevant cases within a data set.
Predictive Analytics	The use of statistics and modelling techniques to determine future outcomes or performance.
RACI Matrix	Illustrates who is Responsible, Accountable, Consulted and Informed within an organisational framework.
Residual Risk	The remaining risk after management has implemented a risk response.
Risk	A measure of the extent to which an organisation is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Factors	Different categories of risk that organisations must consider considered when performing a Fraud Risk Assessment
Rules	Rules used in fraud prevention and detection systems use correlation, statistics, and logical comparison of data to identify a pattern based on insights gained from previous known fraud incidents.
Scams	Where an individual is tricked into making or authorising a payment to a criminal's account. Scammers typically use social engineering and can impersonate banks, investment opportunities, utility companies and government bodies using emails, phone calls and SMS that appear genuine.
Sectorial Anti-Fraud Committee	A committee governed by SAMA to combat fraud involving Member Organisations operating in the Kingdom (e.g., Banking Anti-Fraud Committee).
Senior Management	The highest level of management in an organisation (the level below the Board) and their direct reports.
Service Level Agreement (SLA)	The specific responsibilities for delivery, typically an agreement on timeliness or quality, for example relating to management of fraud alerts.
Static Data	Data with low change frequency (e.g., name, email address, mobile phone number, signatory rights, specimen signatures, power-of-attorney).
The Cyber Security Framework	The Saudi Arabian Monetary Authority Cyber Security Framework.
Third Party	A separate unrelated entity that provides an organisation with a service. This may include suppliers, technology

	providers (e.g., Absher, Nafath), outsourcers, intermediaries, brokers, introducers, and agents.
Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
Trend Analysis	The process of collecting and reviewing information to identify patterns and predict future trends.
Trusted Device	A trusted device is a device that the customer owns, controls access to, and uses often.
Violation	Any act, or concealment of acts, of fraud, corruption, collusion, coercion, unlawful conduct, misconduct, financial mismanagement, accounting irregularities, conflict of interest, wrongful conduct, illegal or unethical practices or other violations of any applicable laws and instructions.
Whistle Blowing Policy	SAMA Whistle Blowing Policy for Financial Institutions.
Wholesale Payment Endpoint Security	Measures taken with respect to endpoint hardware, software, physical access, logical access, organisation and processes at a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem.

Appendix B – Fraud types that may impact a Member Organisation and its customers.

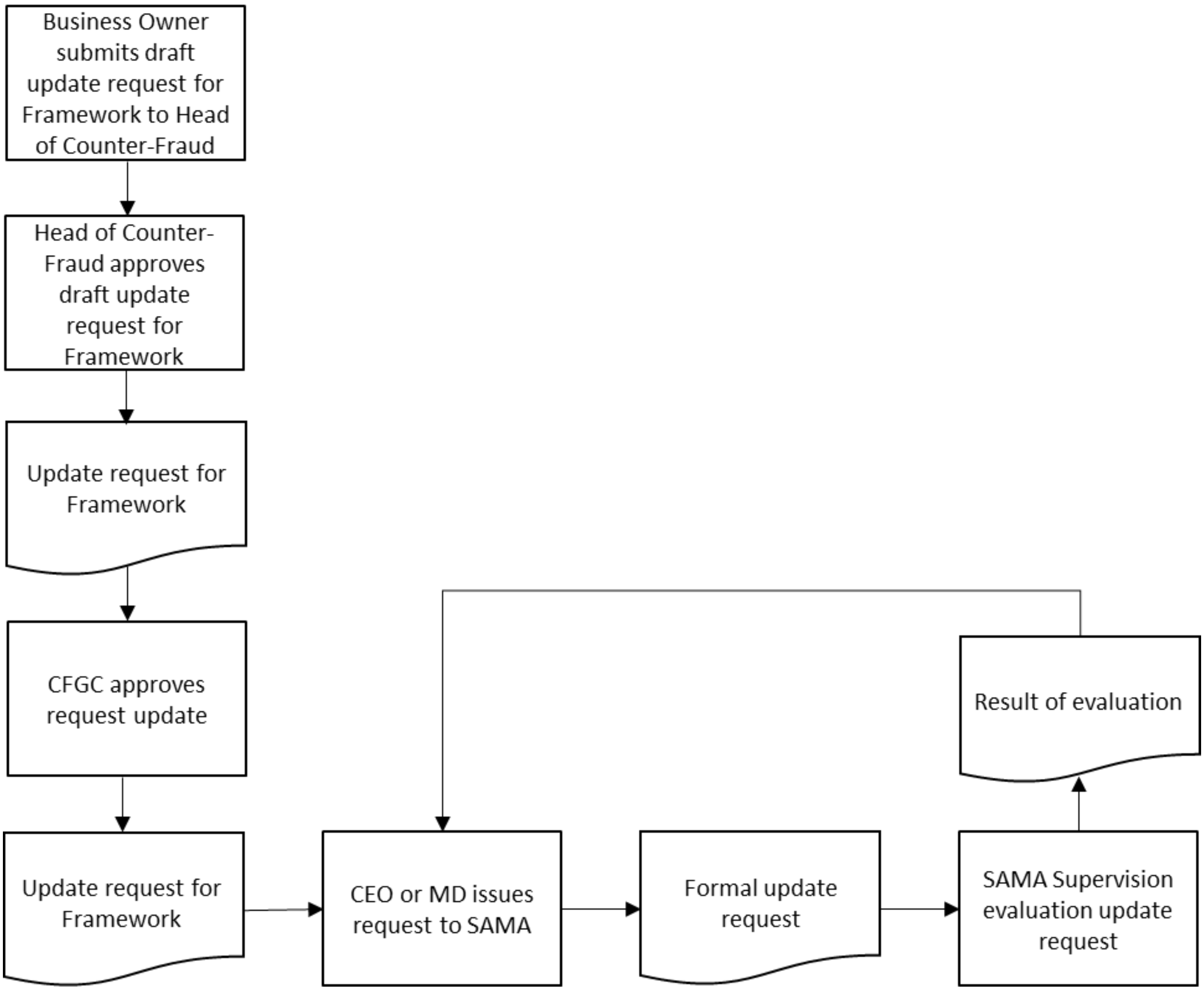
The following is a non-exhaustive list of fraud types that should be considered by a Member Organisation when relevant to its products.

- Social engineering (e.g., capture of customer credentials; investment scams; purchase scams; invoice scams; advance fee scams).
- Account takeover (e.g., gaining access to a customer product or device to control assets or transact).
- Impersonation (e.g., obtaining personal information to use for own benefit; assuming the identity of another to access products; impersonating a government body to obtain customer information).
- Internal fraud (e.g., misappropriation of assets; procurement fraud; theft of assets or cash; theft of intellectual property; falsification of information; unauthorised passing of information to third parties; false expense claims; abuse of authority; collusion; use of organisation assets for own gain; diversion of funds).
- Accounting fraud (e.g., concealment; false invoicing; payroll fraud; improper revenue recognition; overstatement of assets; understatement of liabilities; customer overbilling; treasury and investment fraud).
- Application fraud (e.g., failing to disclose information; falsification of information; providing false documents).
- Wholesale Payment Endpoint Security fraud.
- Banking and payment products: Credit/Debit card fraud; Online or mobile app payment fraud; Cheque fraud; ATM fraud; Mule fraud.
- Credit and lending products: Mortgage fraud; Loan fraud.

Appendix C – How to request an update to the Framework

Below is an illustration of the process for requesting an update to the Framework.

- Detail information supported by pros and cons about the suggested update.
- The request should first be approved by the Head of Counter-Fraud before submitting to the Counter-Fraud Governance Committee (CFGC).
- The request should be approved by Member Organisation's CFGC.
- The request should be sent formally in writing to the manager 'General Department of Cyber Risk Control' via the Member Organisation's CEO or managing director.
- 'General Department of Cyber Risk Control' will evaluate the request and inform the Member Organization.
- The current Framework remains applicable while the requested update is being considered, processed and if applicable is approved and processed.


Business Owner submits draft update request for Framework to Head of Counter-Fraud
Head of Counter-Fraud approves draft update request for Framework
Update request for Framework
CFGC approves request update
Update request for Framework
CEO or MD issues request to SAMA
Formal update request
SAMA Supervision evaluation update request
Result of evaluation

Appendix D – Framework update request form

Request to Update the Counter-Fraud Framework

A submission to the manager of SAMA General Department of Cyber Risk Control.

The Saudi Central Bank (SAMA) will consider requests from a member organisation (MO) to update its Counter-Fraud Framework based on the information submitted using the form below. A separate form must be completed for each requested update. Please note that all required fields must be properly filled in before SAMA will begin the review process

Requestor Information

REQUESTOR'S SIGNATURE* X	REQUESTOR'S POSITION*	DATE*
REQUESTOR'S NAME*	MEMBER ORGANISATION OF REQUESTOR*	

FRAMEWORK SECTION*:
PURPOSE OF REQUESTED UPDATE (including detailed information on its pros and cons)*:
PROPOSAL*:

Approvals

1. MO's HEAD OF COUNTER-FRAUD APPROVAL*	DATE*	
2. MO'S COUNTER-FRAUD GOVERNANCE COMMITTEE APPROVAL*	APPROVER'S POSITION*	DATE*
3. SAMA DECISION	SAMA APPROVAL	DATE

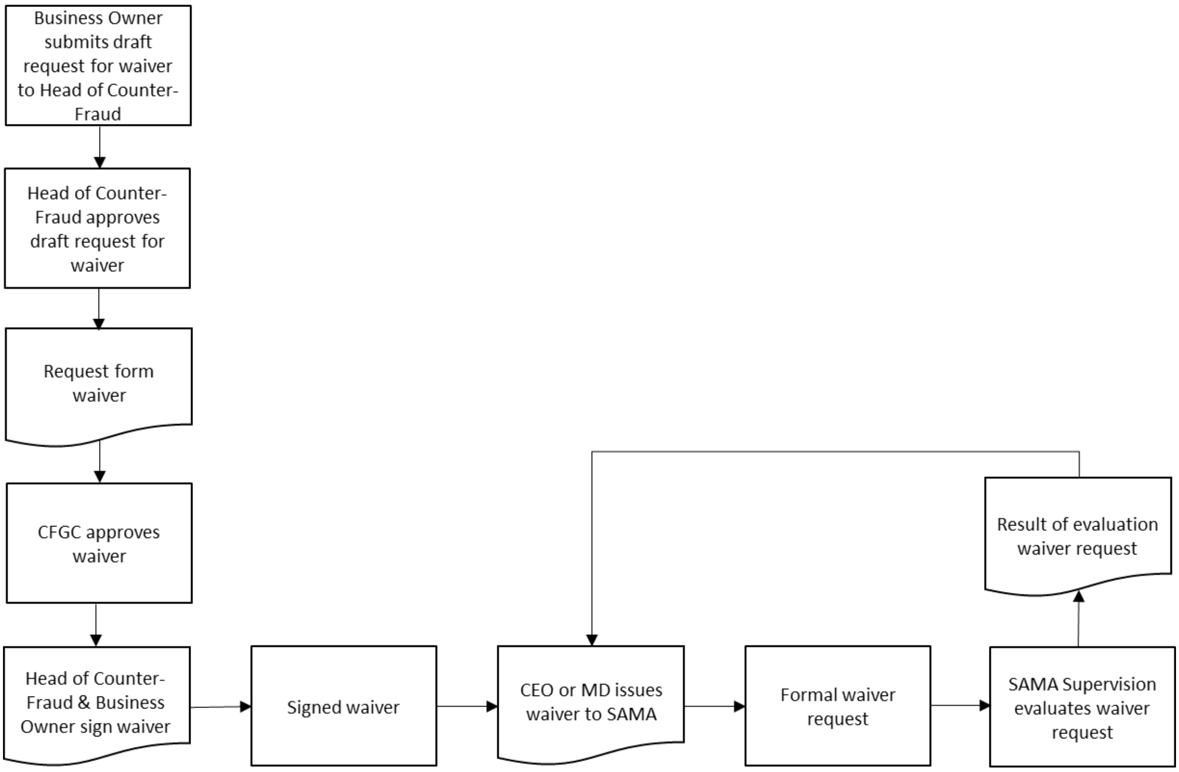
* Denotes required fields

Appendix E – How to request a Waiver from the Framework

Below is an illustration of the process for requesting a waiver from the Framework.

- Detail description about the reasons that the member organisation could not meet the required control.
- Detail description about the available or suggested compensating controls.
- The waiver request should first be approved by the Head of Counter-Fraud before submitting to the Counter-Fraud Governance Committee (CFGC).
- The waiver request should be approved by the members of Member Organisation's Counter-Fraud Governance Committee.
- The waiver request should be signed by the Head of Counter-Fraud and relevant (business) owner.
- The waiver request should be formally issued in writing to the manager of 'General Department of Cyber Risk Control' via the Member Organisation's CEO or managing director.
- 'General Department of Cyber Risk Control' will evaluate the waiver request and inform the Member Organisation.

The current Framework remains applicable while the requested waiver is being evaluated and processed, until the moment of granting the waiver.


Business Owner submits draft request for waiver to Head of Counter-Fraud
Head of Counter-Fraud approves draft request for waiver
Request form waiver
CFGC approves waiver
Head of Counter-Fraud & Business Owner sign waiver
Signed waiver
CEO or MD issues waiver to SAMA
Formal waiver request
SAMA Supervision evaluates waiver request
Result of evaluation waiver request

Appendix F – Framework Waiver request form

Request for Waiver from the SAMA Counter-Fraud Framework
A submission to the manager of 'General Department of Cyber Risk Control'

The Saudi Central Bank (SAMA) will consider requests for waiver from a member organisation (MO) from its Counter-Fraud Framework based on the information submitted using the form below. A separate form must be completed for each requested waiver. Please note that all required fields must be properly filled in before SAMA will begin the review process.

Requestor Information

REQUESTOR'S SIGNATURE* X	REQUESTOR'S POSITION*	DATE*
REQUESTOR'S NAME*	MEMBER ORGANISATION OF REQUESTOR*	

FRAMEWORK CONTROL*:
DETAILED DESCRIPTION OF WHY CONTROL CANNOT BE IMPLEMENTED*:
DETAILED DESCRIPTION OF AVAILABLE OR SUGGESTED COMPENSATING CONTROLS*:

Approvals

1. MO's HEAD OF COUNTER-FRAUD APPROVAL*	DATE*	
2. MO'S COUNTER-FRAUD GOVERNANCE COMMITTEE APPROVAL*	APPROVER'S POSITION*	DATE*
3. SAMA DECISION	SAMA APPROVAL	DATE**

* Denotes required fields
** The validity of this waiver is one year. It is the Member Organisations responsibility to ensure renewal of this waiver.

Appendix G – Supervisor Notification form

Fraud Supervisory Notification

A submission to the manager of SAMA General Department of Cyber Risk Control.

The Saudi Central Bank (SAMA) requires immediate notification of new fraud typologies and significant fraud incidents to mitigate the risk of the fraud impacting additional customers, other organisations, or the financial sector in the KSA. This form should be used to provide the notification. Please note that all required information must be provided, however it is understood that not all information may be available at the time of notification. Where information is not available at the time of notification, any gaps should be supplied to SAMA promptly as the investigation progresses.

Notifier Information

NOTIFIER’S SIGNATURE*	NOTIFIER’S POSITION*	DATE*
NOTIFIER’S NAME*	MEMBER ORGANISATION OF NOTIFIER*	

FRAUD NOTIFICATION TYPE* ☐ New typology ☐ Significant internal fraud ☐ Significant external fraud ☐ Significant accounting irregularity ☐ Wholesale Payment Endpoint Security Fraud	DATE OF INCIDENT*
ORIGIN OF THE INCIDENT*:	
METHODS USED*:	
RELATED PARTIES (INTERNAL AND EXTERNAL)*:	

OUTCOME (INCLUDING LOSSES WHERE APPLICABLE)*:
CORRECTIVE ACTIONS*:
ADDITIONAL INFORMATION:

* Denotes required fields