

Strategi
Compliance

BEST PRACTICE GUIDANCE NOTE

UNDERSTANDING AND MANAGING AML/CFT RED FLAGS

VERSION 3, JULY 2024

Introduction

This Guidance Note is designed to assist Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) compliance officers, directors, senior managers, and staff involved in customer due diligence (CDD) duties. It emphasises the importance of moving beyond mere checklists and adopting a holistic approach to understanding clients. By building comprehensive client profiles and comparing them against standard profiles for their customer type, reporting entities (REs) can effectively use red flags to assess risks. This approach ensures thorough scrutiny and, when necessary, prompts the lodging of Suspicious Activity Reports (SARs) to mitigate financial crime risks effectively.

What is a red flag?

Red flags are indicators that may suggest suspicious activities requiring further scrutiny. They serve as alerts to potential risks and anomalies in customer behaviour or transactions. While a single red flag does not automatically indicate wrongdoing, it prompts a closer examination based on the overall context and customer profile.

Key points to taking a holistic approach to red flags:

- **Context matters:** Evaluate red flags in the context of the customer's normal behaviour and transaction patterns.
- **Know your customer:** Understanding your customer helps differentiate between normal and suspicious activities.
- **Critical questioning:** Internally assess whether the customer's behaviour or transaction aligns with their known profile.
- **Record keeping:** Maintain detailed records of investigations and decisions regarding suspicious activities.

By integrating these key points into your daily operations, including your AML/CFT programme and training efforts, you build a holistic approach to spotting and tackling financial crime risks. This approach not only helps you comply with regulations but also strengthens your business against potential threats, making the financial environment safer overall.



Why should you care about red flags?

Understanding and responding to red flags is key because they serve as a potential indicator of money laundering/terrorism financing (ML/TF). In a demanding work environment where time is limited and client needs are high, it's easy to overlook subtle signs of suspicious activity. Moreover, managing clients who may push boundaries adds further complexity. By remaining vigilant and addressing these warning signs, you protect your professional reputation, secure your business, and promote a safer financial environment overall.

Key reasons:

- **Personal accountability:** Recognising red flags is not just a regulatory duty but a personal responsibility that protects your professional integrity. It ensures that you uphold ethical standards and contribute to a trustworthy financial environment.
- **Business impact:** Vigilance towards red flags helps shield your business from reputational harm and potential financial losses associated with illicit activities. It safeguards client trust and enhances the credibility of your services.
- **Legal consequences:** Failing to detect and report suspicious activities can lead to legal repercussions, including fines and regulatory sanctions. Compliance with red flags is essential for mitigating these risks and maintaining operational stability.

By prioritising red flags, you actively safeguard your career, protect your business interests, and uphold the integrity of the financial sector as a whole. It's about staying vigilant and accountable in the fight against financial crime.

What should you do if you discover a red flag?

Upon identifying a red flag:

- **Investigate:** Take the time to conduct a thorough internal investigation. This means gathering additional information and context to understand the situation better. For example, reviewing transaction details or customer interactions can provide insights into potentially suspicious activities.
- **Ask critical questions:** Evaluate whether the flagged activity aligns with the customer's known profile and expected behaviour. For instance, if a customer suddenly engages in transactions significantly outside their typical pattern, it warrants closer scrutiny.

> **Tip:** Ask yourself privately, "Given what we know about this customer, does this transaction make sense?" Consider the customer's profile, transaction details, and identified risks. If it doesn't add up, it may be time to start identifying suspicious activity and preparing a report.

- **Review documentation:** Ensure all customer information and transaction records are current, accurate, and readily accessible. This step is crucial for piecing together a complete picture of the customer's history and activities.

- **Analyse the risk profile:** Compare the customer's current activities with the standard risk profile outlined in your organisation's AML/CFT programme. This comparison helps assess the risk level associated with flagged behaviours, such as sudden increases in transaction size by a client. This comparison ensures that you're following your organisation's rules and regulatory requirements, helping you manage risks effectively and stay compliant.
- **Document decisions:** Maintain detailed records documenting your findings and the reasoning behind any decisions made regarding the flagged activity. This documentation is essential for demonstrating compliance with regulatory requirements and internal policies.

Tip: It's important to keep thorough records when conducting internal investigations. When the Financial Intelligence Unit (FIU) reviews a suspicious activity report, they might request additional information. Detailed records help the FIU understand why the report was filed. Similarly, if a decision is made not to file a report due to uncertainty, detailed records can justify this decision, especially if other entities reported similar activities.

- **File a SAR if warranted:** If your investigation substantiates suspicions of illicit activity, promptly file a Suspicious Activity Report (SAR) with the Financial Intelligence Unit (FIU). SARs are crucial for reporting suspicious transactions and ensuring appropriate actions are taken to mitigate financial crime risks. You don't have to prove ML/TF. All you need is a reasonable basis for forming a suspicion.

Steps to filing a SAR:

1. **Identify suspicious activity:** Recognise transactions or behaviours that deviate from the customer's normal pattern.
2. **Gather information:** Collect pertinent details such as transaction specifics and customer information.
3. **Complete the SAR form:** Use the official SAR form provided by the FIU, ensuring all sections are accurately completed.
4. **Submit the SAR:** File the completed SAR through the designated secure channel- GOAML.
5. **Maintain confidentiality:** Safeguard the SAR and related information, sharing only with authorised staff.

Tip: Remember, a SAR is confidential, and should only be discussed with a select few. It should not be discussed with the customer.

6. **Follow up:** Be prepared to provide additional information or clarify details as requested by the FIU.

Each organisation will have its own process documented in their AML/CFT programme, outlining specific procedures for filing a SAR effectively.

Types of red flags

Red flags encompass various indicators across sectors that may suggest potential suspicious activities. These indicators generally fall into sixmain categories:

1. Customer red flags

Examples include:

- Politically Exposed Persons (PEPs) or high-net-worth individuals.
- Known connections to criminals.
- Subject to sanctions.
- Involved in media reports related to crimes like drug trafficking or human trafficking.
- Presenting fake documents or using anonymous names.
- Using identities that have previously been flagged.
- Previously reported in a suspicious activity report (SAR).

2. Behaviour red flags

Examples include:

- Frequent changes in professional service providers within a short timeframe.
- Previously denied similar services elsewhere.
- Reluctance to comply with customer due diligence (CDD) requirements.
- Lack of supporting documentation for claims or requests.
- Avoidance of direct contact or sudden change in communication preferences.
- Urgency to complete transactions without reasonable explanation.
- Willingness to overpay for services.
- Significant and unexplained changes in risk, social, or economic profiles.
- Engaging intermediaries without clear rationale.
- Attempts to avoid providing identity documentation.
- Visible signs of nervousness or apprehension.



3. Structure red flags

Examples include:

- Use of shell companies or complex legal structures without clear economic or lawful reasons.
- Frequent changes in beneficial ownership to evade scrutiny.
- Secrecy surrounding identity or structure of legal entities.
- Difficulty in understanding or verifying beneficial ownership.
- Lack of documentation supporting beneficial ownership.
- Use of nominees or trusts without valid justification.
- Instructions from unrelated parties or professionals.
- Spanning multiple jurisdictions without clear economic or lawful purpose.

4. Transaction red flags

Examples include:

- Transactions inconsistent with the customer's known activities or sector norms.
- Funds from unrelated accounts or unexplained sources.
- Unusual sources of funds that are difficult to trace or verify.
- Sudden urgency in transaction requests without justification.
- Unexpected refunds or deposits into trust accounts.
- Unexplained changes or cancellations in transactions.
- Requests to redirect refunds to different accounts.
- Deposits exceeding transaction values without clear reasons.
- Structured payments to avoid reporting thresholds.
- Back-to-back transactions increasing in value.

5. Geographic red flags

Examples include:

- Engaging services from distant locations without apparent reasons.
- Seeking services not available in their domicile country.
- Requests for services in locations different from the reporting entity's base.
- Transactions involving funds from high-risk or sanctioned jurisdictions.
- Involvement of customers from countries known for high-risk activities like human trafficking or drug trafficking.

6. Source of wealth/Source of funds red flags

Examples include:

- Inconsistencies in economic profiles without plausible explanations.
- Significant cash deposits without clear source or purpose.
- Unverifiable source of wealth or funds.
- Multiple bank accounts or foreign bank accounts without lawful reasons.

Your organisation's AML/CFT programme is your first port of call for identifying red flags. Make sure your list is up to date to effectively manage risks and meet regulatory requirements.

Sector-specific red flags

Each sector has its own set of unique red flags outlined in sector-specific risk assessments. While a general understanding of red flags is essential, it's important to recognise that specific sectors may present distinct indicators.

For example, in real estate:

- Lack of interest in typical property features like school proximity or transit access.
- Swift purchase and resale of properties before legal ownership updates.
- Purchasing property without physically viewing it.

In financial advice:

- Indifference towards fee structures associated with products or services.
- Specific focus on cancellation policies and associated fees.

> **Tip:** The Department of Internal Affairs (DIA) and Financial Markets Authority (FMA) publish comprehensive guidance and sector risk assessments. Accessing this information is straightforward through the DIA's website, which lists all supervised sectors, and the FMA's 2021 sector risk assessment available online, particularly Section 8 detailing supervised sector risks.
>
> Additionally, consider incorporating Strategi's sector-specific training into your programme for key staff. This training is highly valued and can enhance your team's ability to identify and respond to sector-specific risks effectively.



Training your team

Training staff to effectively identify and respond to red flags is probably the most important thing a business can do to maintain compliance and safeguard against financial crime risks.

Here's how you can ensure your team is well-prepared:

Comprehensive training: Conduct regular training sessions that cover:

- **Red flag recognition:** Educate staff on recognising indicators of suspicious activities, including sector-specific red flags.
- **Reporting procedures:** Train them on the correct procedures for documenting and reporting suspicious activities, emphasising the importance of accuracy and completeness in SAR filings.
- **Compliance responsibilities:** Ensure staff understand their roles and responsibilities in adhering to AML/CFT regulations and maintaining organisational integrity, which also protects their professional reputation.

Role-specific training: Tailor training programmes based on job functions and exposure to AML/CFT risks. For example:

- **Customer-facing roles:** Provide specific guidance on conducting enhanced due diligence (EDD) and managing relationships with high-risk customers.
- **Back-office staff:** Focus on transaction monitoring techniques and recognising unusual patterns or behaviours in financial transactions.

Training frequency

- **Initial training:** Conduct comprehensive training sessions for new hires to familiarise them with AML/CFT policies, red flags, and reporting obligations from the outset.
- **Ongoing training:** Schedule regular refresher courses at least annually to reinforce knowledge and update staff on regulatory changes, emerging threats, and sector-specific risks.
- **Adaptability:** Encourage staff to remain adaptable and responsive to evolving regulations and industry best practices.

> **Tip:** Encourage your team to openly ask questions about red flags. This helps create a supportive environment where everyone feels comfortable seeking clarity and understanding potential signs of suspicious activity.

By investing in staff training, including sector-specific insights such as those outlined in the DIA and FMA risk assessments, you equip your team with the knowledge and skills needed to detect and mitigate financial crime risks effectively. Incorporating Strategi's sector-specific training can further enhance your staff's expertise, ensuring they stay ahead of potential threats in their respective roles.

Penalties and risks of missing a red flag

Failing to spot and address red flags can have serious consequences:

- Legal penalties: You could face hefty fines and legal action for not following AML/CFT rules.
- Reputational damage: Losing trust, missing out on business opportunities, and harming your brand and reputation.
- Operational risks: Unintentionally aiding criminal activities, leading to disruptions in operations and financial losses.

The AML/CFT Supervisors want reporting entities to take a risk-based approach. A key to a risk-based approach is building client profiles, risk rating clients and being aware of red flags.

Key resources

Strategi:

- **Subscribe Strategi's monthly AML/CFT newsletter.**
- **AML/CFT compliance officer (Micro-credential) (Level 4).**
- **Guidance Note: AML/CFT new regulations June 2024.**
- **AML/CFT review service.**
- AML/CFT sector specific webinar - contact us.

AML/CFT Supervisors:

- **Department of Internal Affairs AML/CFT news and updates.**
- **Financial Markets Authority news and updates.**
- **Financial Markets Authority – risk assessment guideline.**

New Zealand Police (SAR:

- **Suspicious activity and transaction reports.**

Conclusion

Remember, spotting and responding to red flags isn't just about following rules—it's about understanding your clients holistically. By taking this approach, you not only protect your business and clients but also safeguard one of the most important things—your own professional reputation. Stay vigilant, stay informed, and keep building trust with your clients.

Strategi
Compliance

BEST PRACTICE GUIDANCE NOTE

UNDERSTANDING AND MANAGING AML/CFT RED FLAGS

For more information contact:

David Greenslade BA, MBA, Dip Mgt, Dip Bus Studies (PFP), MIML, MInstD, AFA

Executive Director

M: +64 21 400 600

E: david.greenslade@strategi.co.nz

W: strategi.co.nz

Disclaimer: The authors, consultants, editors plus the directors and staff of Strategi Limited and Strategi Institute Limited expressly disclaim all and any liability and responsibility to any person, whether a purchaser or reader of this publication or not, in respect of anything, and of the consequences of anything, done or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication. Any examples that may be provided in the guidance note are only to explain our approach and these are not exhaustive. This guidance note is not and does not constitute legal advice. The reader is recommended to seek independent legal advice if required.

17e Corinthian Drive, Albany, Auckland 0632

PO Box 301426, Albany, Auckland 0752, New Zealand

Telephone +64 9 414 1300 | Email compliance@strategi.co.nz

STRATEGI.CO.NZ

ADVICE YOU CAN PROFIT FROM