THE TA FORUM
AML Working Group

Identification and Assessment of Financial Crime Risks

Introduction

Firms must ensure they have measures in place to identify potential financial crime risks to its customers and business. These measures should be proportionate and implemented based on an assessment of risk.

FCA SYSC 6.3 – Financial Crime

SYSC 6.3.1 R
A firm must ensure the policies and procedures established under SYSC 6.1.1 R include systems and controls that:

(1) enable it to identify, assess, monitor and manage money laundering risk; and

(2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

SYSC 6.3.2 G
"Money laundering risk" is the risk that a firm may be used to further money laundering. Failure by a firm to manage this risk effectively will increase the risk to society of crime and terrorism.

SYSC 6.3.3 R 01/04/2009RP
A firm must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to comply with SYSC 6.3.1 R.

Assessment of Risk

The FCA's Financial Crime Guidance includes the following information with regards to Financial Crime risk assessments:

"A thorough understanding of its financial crime risks is key if a firm is to apply proportionate and effective systems and controls. A firm should identify and assess the financial crime risks to which it is exposed as a result of, for example, the products and services it offers, the jurisdictions it operates in, the types of customer it attracts, the complexity and volume of transactions, and the distribution channels it uses to service its customers. Firms can then target their financial crime resources on the areas of greatest risk."

A firm will assess its overall exposure to money laundering risks based on

(1) its customer, product and activity profiles;

(2) its distribution channels;

(3) the complexity and volume of its transactions;

(4) its processes and systems; and

(5) its operating environment.

In addition to this there will also be specific financial crime risks that a firm may be exposed to. These risks would usually be recorded within a firm's Risk Register.

A firm should regularly review and assess its risks as these may be subject to change due to a number of factors. These factors could include changes in business model, product offerings or emerging risks within the industry. It may also be prudent to seek an external opinion on the firm's risk assessment from time to time.

Each risk should be identified and assessed with regards to its impact if the risk were to materialise, and the likelihood of it occurring with the mitigation controls currently in place. This enables a firm to produce a risk score to identify those risks that present areas of concern. These risks may then require additional controls to be implemented or existing controls to be changed to reduce the likelihood of the risk occurring.

The scoring methodology can vary from firm to firm. Some possible considerations are:

Impact – Customer, Financial, Regulatory, Reputational

Impact Severity – Minor, Moderate, Major, Extreme, Catastrophic

Likelihood – Rare, Unlikely, Possible, Likely, Almost Certain.

Each firm will set its own thresholds/criteria for the impact and likelihood categories.

It can be the case that when assessing risks some risks are accepted by a firm due to its risk appetite. It is unlikely however that any Financial Crime risk would fall into this category.

Risk indicators

Some indicators that may reflect a materialising risk can be an increase in complaints with regards to a certain process or area of the business, an increase in breaches and near misses and an increase in Suspicious Activity Reports.

Ownership of Risks

Each risk should have an owner responsible for reviewing the risk score on a regular basis and updating the mitigating controls as and when they change.

Ongoing monitoring

The risk owner and where in place, the Risk Committee, should conduct ongoing monitoring of all risks across the business to identify emerging or materialising risks and put into place mitigation controls wherever possible.

Effectiveness reviews of existing controls

Existing controls should be reviewed for effectiveness on an ongoing and risk-based approach. These reviews can be undertaken via a variety of methods such as:

- Compliance monitoring findings and feedback
- Breach and Complaints data
- Quality Assurance results data
- External Audit findings and recommendations
- Industry best practice publications

Risk Reporting

Risk Management Information (MI) should be produced on a regular basis. This could include such information as:

Number of risks across the business
Number of risks per business area
Number of risks rated as “low”
Number of risks rated as “medium”
Number of risks rated as “high”
Risks that have a high likelihood of occurring
Risk ratings that have changed since the last reporting date
Controls that have changed since the last reporting date
Anything that needs to be highlighted or escalated

This MI should be provided to all risk owners, the Risk Committee and the Board. The Board is ultimately responsible for monitoring risks within the business.

Potential Risks – **The table below details some examples of potential financial crime risks that a firm may face and possible mitigation. (This list is not exhaustive; firm’s may also identify additional risks and risks specific to their type of business).**

Category	Risk	Possible Mitigation*
Fraud	Internal Fraud	Segregation of duty. Bank authorisation levels. Minimum of 4 eye checking. Safe / lockbox to store cheques. Conflicts of interest. declarations & register. Membership of industry groups/forums and participation in Fraud alert schemes.
Fraud	External Fraud – Account takeover	AML verification. Bank account verification. Data Protection checks. Minimum of 4 eye checking. Membership of industry groups/forums and participation in Fraud alert schemes.
Fraud	External Fraud – Invoice fraud	Minimum of 4 eye checking Senior Management Sign off. Telephone call to requester to confirm payment. Membership of industry groups/forums and participation in Fraud alert schemes.
Fraud	Corporation Impersonation Fraud	Frequent web searches. Use of specialist company to search for and identify brand impersonation. Use of Companies House email alert system to notify changes to corporate information. Use of Companies House PROOF scheme to protect from fraudulent filings. Membership of industry groups/forums and participation in Fraud alert schemes.
Money Laundering	Failure to identify money	Customer risk rating.

	laundering	AML checks. PEP and Sanctions checking. Minimum of 4 eye checking. Suspicious Activity Reporting. Trigger event checks. Transaction Monitoring.
Sanctions	Sanctions identification failure	Sanction screening system. Escalation procedures. System flags and Freezing capabilities.
Politically Exposed Persons	Politically Exposed Persons (PEP) identification failure	PEP checking system. Escalation procedures. System flags.
Enhanced Due Diligence	Failure to apply Enhanced Due Diligence when required	Customer risk rating. Transaction Monitoring. PEP checking system. System flags.
Cyber Crime	System attack	Use of reputable IT provider with ISO Certification. Regular penetration testing. Spam filters.
Cyber Crime	Phishing emails	Use of reputable IT provider with ISO Certification. Regular penetration testing. Spam filters. Spam email receipt escalation process.
Tax Evasion	Failure to identify Tax Evasion	Self-certification & AEOI reporting. Customer risk assessment. System flags. Escalation of payments to high-risk countries. Bank verification tools.
Terrorist Financing	Risk that the firm is used to facilitate Terrorist financing	PEP and Sanctions checking. Customer risk assessment. AML Verification. Transaction monitoring. Escalation of links to high-risk countries and industries. Suspicious Activity Reporting.
Bribery and Corruption	A member of staff offers or accepts an inducement	Gifts and Hospitality procedures and logs.

		Expense payments reviews. Conflicts of Interest declarations and register.
Market Abuse	Staff fail to seek pre-approval of, or post notification of, personal investment transactions where required	Personal Account Dealing procedures and logs. Conflicts of Interest declarations and register. Transaction Monitoring.
Suspicious Activity	Failure to report Suspicious Activity	Suspicious Activity Reporting procedures. Transaction Monitoring. Risk Assessments. System Flags.
Pension Transfer Scams	Failure to Identify a Pension transfer Scam	Compliance referrals for Pension Transfers. Communication with client prior to transfer.

***Note: there are some examples of generic mitigation that will be applicable across all risks such as; Staff Training and Awareness, Documented Procedures and Compliance Monitoring.**