
Overview

This standard is about identifying potential crime within your organisation. You must monitor transactions and other business activities to identify potential financial crime, within your organisation. You must have all of the relevant information at your disposal to allow you to make accurate and informed judgements about the activity you are monitoring and to identify potential financial crime and respond to actual crystallised events.

This standard is relevant to roles in countering financial crime.

Performance criteria

You must be able to:

1. keep up-to-date with financial risk indicators, typologies, surveillance and prevention and detection methods
2. identify effective management information to identify actual financial crime events within your organisation
3. develop effectiveness management information where none exist
4. analyse the root causes of financial crime events
5. develop and maintain an awareness of usual business activity, employee and client behaviour as appropriate
6. monitor client, employee and third party supplier behaviour and business activity on a regular basis to identify unusual occurrences
7. observe relevant boundaries of confidentiality and data security when monitoring business activities and transactions
8. ensure you have access to all available information that will enable you to detect potential financial crime
9. assess transactions and business activity against employee, client and other business information available to you
10. accurately identify the type and nature of suspicious activity or potential financial crime
11. escalate your findings as appropriate following internal procedures

Knowledge and understanding

You need to know and understand:

1. your organisation's strategy and approach towards countering financial crime
2. what might be regarded as suspicious or potentially suspicious activity
3. how to identify actual financial crime events
4. procedures for detecting potential financial crime such as monitoring systems
5. usual client/third party behaviour and how to identify deviations from this
6. boundaries/remit of your authority in monitoring business activity
7. information that you are permitted to obtain and use to detect potential financial crime
8. how to undertake financial crime investigations in your organisation
9. records that need to be maintained, how this should be done and the relevant procedures to follow
10. procedures for escalating and reporting crime, both internal (e.g. whistle blowing) and external
11. your organisation's disciplinary process and procedures
12. relevant records required and how these should be maintained
13. the legislation, regulations and codes of practice, relevant to you and your organisation and any specific obligations

Glossary

Empowered Authority

This is any individual or authority that is legally entitled to make a request of your organisation. This most often takes the form of a request for information and in the cases of financial crime is likely to originate from a law enforcement agency or regulator.

Financial Crime

This includes any offence involving money laundering, terrorist financing, fraud or dishonest or market abuse. (Definition based on the FCA definition of financial crime). This includes financial crime both internal and external to a financial services organisation.

Legal and regulatory requirements

This refers to a range of obligations incumbent upon financial organisations and is commonly referred to as 'compliance' requirements. The legal and regulatory requirements of an organisation or individual/s within it (such as 'approved persons') may differ slightly according to the type of financial organisation and the services it offers. The regulator of all providers of financial services in the UK oversees a number of regulated activities under powers derived from the Financial Services and Markets Act 2000.

A number of other pieces of UK legislation are relevant to the countering of financial crime, such as the Proceeds of Crime Act (POCA), the Serious Organised Crime and Police Act (SOCPA), the Fraud Act 2006, for example. UK financial institutions are also subject to European Commission legislation enacted by the British Government such as the Market Abuse Directive and the Basel 2 Accord (for capital adequacy).

Financial organisations, like any other employer, are also subject to a range of legal requirements covering areas such as discrimination, equality and diversity, Health and safety and Data protection.

Organisation

This refers to an organisation that offers financial services – this could be insurance, investment, lending and credit, pensions, securities and derivatives. It includes organisations in both the public and private sector.

Systems and controls

The practices and procedures put in place to protect an organisation from financial crime. In some cases it is accepted that certain (or indeed all) types of financial crime cannot be wholly prevented, but controls can limit its extent and impact.

Crystallised event

the risk has materialised and the controls that were in place to deal with the risk were found to be ineffective. This would prompt a review of the controls and re-testing to ensure the risk cannot happen again

FSPCFC8

Identify potential financial crime within your organisation



Developed by	FLSP
Version Number	2
Date Approved	January 2016
Indicative Review Date	January 2021
Validity	Current
Status	Original
Originating Organisation	Financial Skills Partnership
Original URN	FSPCFC8
Relevant Occupations	Financial Institution and Office Managers; Financial institution managers
Suite	Countering Financial Crime
Keywords	Financial crime; crytalisised events; transactions; monitor
