



How to address the FCA'S "Dear CEO" letter on anti-money laundering framework weaknesses

Practical advice to assess the efficiency of your anti-money laundering (AML) framework

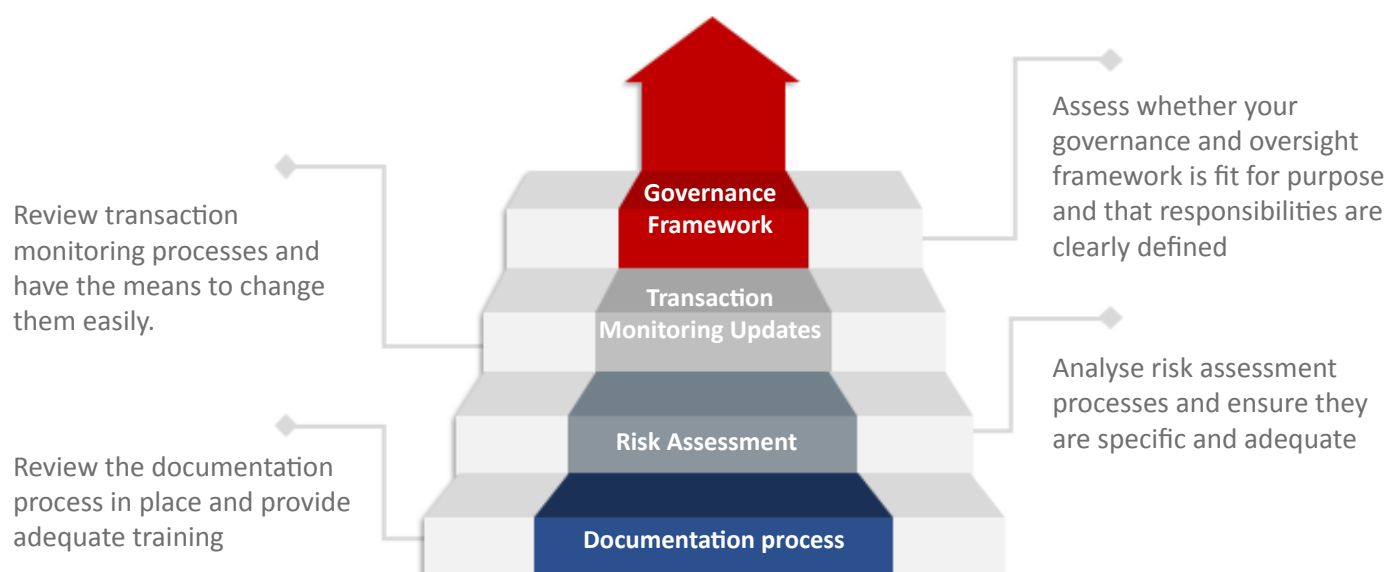


INTRODUCTION

In June, the Financial Conduct Authority (FCA) published its “Dear CEO” letter, which was originally sent to retail banks on the 22nd of May 2021. In it, the authority enumerates the common weaknesses they identified during their recent assessment of retail banks’ financial crime systems and controls. Additionally, the FCA orders banks to demonstrate more efforts to address persistent AML framework failings and instructs them to complete a comprehensive gap analysis of all AML weaknesses by the 17th of September 2021. If mitigation plans are not implemented to close the gaps revealed by the analysis, banks could face serious regulatory interventions. While this letter is addressed to retail banks, all other bank types, such as corporate bankers and investment banking firms, are advised to use the regulator’s findings to assess and consider the effectiveness of their financial crime controls.

To help you understand the FCA’s request, RedCompass Labs prepared a summary of the letter, which you can read [here](#). Considering the immense pressure banks are under, particularly with the deadline rapidly approaching, we are taking a step further to support you and share four areas to analyse when conducting the assessment of your AML frameworks, as well as some potential ways to address failings in the following areas:

- Process documentation and training
- Risk assessment processes
- Transaction monitoring processes
- Governance framework



01

Documentation process

Review the documentation process in place and provide adequate training

All compliance processes (e.g., KYC, CDD, EDD, SARs, etc.) must be documented and communicated to the relevant staff. Your employees need to know in detail the robust processes in place, and more specifically, the steps they need to take in the event of suspicious activities. They also should be fully acquainted with how to manage high-risk customers.

For your staff to be familiar with the compliance processes and avoid gaps and potential breaches in this area, financial crime training should be run regularly. These sessions must remind staff of the existing measures in place, list new threats and typologies, and share early enough any changes implemented on the AML framework resulting from these new trends.

02

Risk Assessment

Analyse risk assessment processes and ensure they are specific and adequateadequate training

Both business-wide and customer risk assessment processes must be very specific and well understood. They should address all relevant financial crime risks considered on a domestic and global scale. Unfortunately, some threats are often not considered or overlooked by the risk assessment framework. For example, signs of modern slavery and human trafficking generally sits outside of the framework's remit. When addressing the FCA's Dear CEO letter, all the 22 offences listed in the **6AMLD** regulations should be considered, regardless of the fact that the UK has opted not to adopt this directive.

If you do not have the expertise in-house, and therefore the adequate controls in place, consider integrating your data set with external sources like RedCompass Labs **RedFlag Accelerator**. This is the most comprehensive set of modern slavery, human trafficking and child sexual exploitation red flags powered by a cutting-edge data investigation and analytics platform.

In the same fashion, processes outsourced to a third party providing expertise or technology are also often mistakenly considered out of scope. In fact, they should be fully analysed and, most importantly, understood by your staff too.

03

Transaction Monitoring

Review transaction monitoring processes and have the means to change them easily.

With new threats constantly emerging, it is critical that the procedures and systems in place are continuously re-calibrated to remain in line with your bank's risk profile, business model, products and customer base.

For this to happen, verify that your framework allows you to fine-tune your transaction monitoring system easily. If this is a challenge, consider utilising technology like RedCompass Labs **D1R4FinCrime** as a mitigation action. It will give you the ability to rapidly modify the ruleset while providing the transparency called for by the FCA. Concerned with an overreliance on out-of-the-box controls and rules, the FCA will expect your staff to be able to explain the technical setup, rules and processes of your transaction monitoring systems.

04

Governance Framework

Assess whether your governance and oversight framework is fit for purpose and that responsibilities are clearly defined

For the anti-money laundering framework to be efficient, each party must clearly understand the division of accountability between the first and the second lines of defence. There should be no room for assumptions.

Similarly, senior management should clearly understand:

- the risk assessment process and, more particularly, how a risk qualifies as low, medium, or high
- the sign-off process that goes along with that assessment

If the analysis reveals that this process is not perfectly clear, the oversight framework should be reviewed. In case of a lack of resources internally, a professional services firm can be involved in this process to provide the required perspective and the change management techniques necessary when adjusting these complex frameworks.

CONCLUSION

Hopefully, these practical steps will help you to meet the deadlines set by the FCA. We know that this FCA request is not easy to address, let alone within such short timelines. However, if you need support or don't have enough resources to allocate to this complex exercise, RedCompass Labs can help you review, assess and improve your anti-money laundering framework. In fact, the four practical considerations shared in this whitepaper are part of the RedCompass Labs **FastStart analysis** framework. This service has been designed to undertake the assessment demanded by the FCA and to provide suggestions for improvement within a very short timeframe. If you want to know more, please feel free to reach out.



About RedCompass Labs

RedCompass Labs helps financial institutions deliver profitable, secure, end-to-end payment and financial crime services and solutions.

The team provides advanced AI data-led payments and financial crime testing technology, data analytics services together with delivery-focused consulting, managed services, and world-class workshops on a vast array of subjects, including the Future of Payments and **ISO 20022**.

RedCompass Labs is committed to opening the doors of finance to all with our payment expertise and data-led technologies, and protecting those who enter, especially by disrupting financial crime that affects the most vulnerable. To this end, we have invested in R&D, data science and created **DIR4Payments**, a game-changing way to accelerate, lower cost and increase coverage by using production data for payment platforms.

We have also developed the RedCompass Labs RedFlag Accelerator, the global point of reference of modern slavery, human trafficking, and Child Sexual Exploitation red flags for the financial industry. The RedFlag Accelerator won the PayTech For Good Award and Themis Anti Financial Crime Innovation Award. Today, RedCompass Labs supports its clients from its four offices in London, Singapore, Tokyo, and Warsaw.

Don't hesitate to contact us if you need support.

We can provide:

MSHT & Child Sexual Exploitation:

- FastStart Analysis
- Investigation Services and Monitoring

Fraud and Sanctions, AML System

- Tuning & Test
- Upgrade Delivery



[@RedCompass Labs](https://www.linkedin.com/company/redcompasslabs)



[RedCompass1](https://twitter.com/RedCompass1)



www.redcompasslabs.com



[RedCompass Labs](https://www.youtube.com/RedCompass Labs)