## 

## 

## 

## 

[COMPANY NAME] MLRO Report, [DATE]

## Prepared by [NAME], [TITLE]

## 

## How to use this template *[DELETE THIS SECTION]*

This document can be used as either a template or a reference for creating your annual Money Laundering Reporting Officer (MLRO) report. The MLRO report can be utilised by the MLRO and other senior members within compliance and risk functions.

MLROs play a critical role and are required to satisfy the compliance oversight function (SMF16) and money laundering reporting function (SMF17) under the Financial Conduct Authority (FCA). Many MLROs have past background and experience within compliance, legal and other areas within financial services. MLROs are required to complete relevant training courses and continue to maintain an adequate understanding of current regulatory rules and expectations.

Firms should have an appointed MLRO position prior to seeking authorised and registered status within the FCA.

For more details about the MLRO function, please refer to [FCA guidance](https://www.fca.org.uk/firms/approved-persons/heads-compliance-mlro-applicant-competency-capability).

We’ve included recommended sections, *guidance text in italics*, some starter text you can directly edit and include, and some tables for you to populate.

You’ll also find some charts in the template. The data for these charts can be found in the accompanying spreadsheet. By entering your own data in the spreadsheet, the charts are automatically updated to represent your data to show the effectiveness of your own controls.

Table of Contents

[Prepared by [NAME], [TITLE] 1](#_Toc94789480)

[How to use this template [DELETE THIS SECTION] 2](#_Toc94789481)

[1. Introduction 4](#_Toc94789482)

[2. Summary and Conclusion 4](#_Toc94789483)

[3. MLRO Recommendations and Objectives 4](#_Toc94789484)

[4. Financial Crime Journey 5](#_Toc94789485)

[4.1. Growth of the Business 5](#_Toc94789486)

[4.2. Growth and Evolution of the Team 5](#_Toc94789487)

[4.3. New Products / Features 5](#_Toc94789488)

[5. Financial Crime Framework 6](#_Toc94789489)

[5.1. AML Governance Framework 7](#_Toc94789490)

[5.2. Financial Crime Structure 8](#_Toc94789491)

[5.3. Governance Committee Structure 8](#_Toc94789492)

[6. Systems and Control Effectiveness 9](#_Toc94789493)

[6.1. Staff Training 9](#_Toc94789494)

[6.2. Management Information (MI) 11](#_Toc94789495)

[6.3. Senior Management Oversight 15](#_Toc94789496)

[6.4. Policies and Procedures 15](#_Toc94789497)

[6.5. Risk Assessment 16](#_Toc94789498)

[6.6. Assurance 17](#_Toc94789499)

[7. Overview of [INSERT Business Area - i.e., business banking, merchant services, crypto wallet] 19](#_Toc94789500)

[7.1. Growth / KPIs 19](#_Toc94789501)

[7.2. Summary of Controls 19](#_Toc94789502)

[7.3. Key Milestones and Areas of Concern 19](#_Toc94789503)

[7.4. Onboarding Controls 20](#_Toc94789504)

[7.5. Effectiveness of Screening 23](#_Toc94789505)

[7.6. Effectiveness of Customer Risk Rating 30](#_Toc94789506)

[7.7. Effectiveness of Customer and Enhanced Due Diligence 32](#_Toc94789507)

[7.8. Financial Inclusion 33](#_Toc94789508)

[7.9. Effectiveness of Ongoing Monitoring 34](#_Toc94789509)

[7.10. Suspicious Activity Reporting 37](#_Toc94789510)

### Introduction

*This section typically includes standard content about how this report meets the regulatory requirements. You may also wish to clarify the scope of the report - for example, that it includes the opinion and conclusion of the MLRO as well as specific recommendations to resolve issues. It also may be helpful context to share how these conclusions were reached - were there external findings, use of data, personal interactions with the business, etc.*

The purpose of this report is to provide senior management with a clear view of the effectiveness of the financial crime framework and meet the firm’s obligation under the Senior Management Arrangements, Systems and Controls (SYSC) requirement 3.2.6G (2). Firms are required “to ensure that the systems and controls include…appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's money laundering reporting officer (MLRO) on the operation and effectiveness of those systems and controls”.

The scope of this report covers management information and the recommendations of the MLRO regarding [BUSINESS AREAS], across [YEAR]. The opinion and conclusion was achieved through data, internal and external assurance and regular interactions with the business.

### Summary and Conclusion

*This section should include an overall evaluation of the state of the financial crime systems and controls, answering the core question “are they effective”. Put another way, if this is the only thing senior management read - what do they most need to know about the state of things? It should also cover key milestones and issues - what’s gone particularly well this year, what are you most concerned about, and what’s changed. For example, if the business has recently experienced significant growth, you may want to call out that your approach to transaction monitoring is no longer appropriate for the size and scale of the business.*

### MLRO Recommendations and Objectives

*At a high level, what do you hope happens as a result of this report? What do you need to ensure that your systems and controls are effective? This is your opportunity to make recommendations to improve your management of financial crime risks, including any need for resources.*

The recommendations from this MLRO report are detailed in the table below. We believe that a period of [INSERT] will be required in order to effectively implement these solutions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference Number** | **Recommendation** | **Owner** | **Due Date** |
| # |  |  |  |
| # |  |  |  |
| # |  |  |  |

### Financial Crime Journey

*This section is most useful for fast growing businesses and gives you a chance to highlight how the financial crime programme has evolved to keep up with the growing business. We have included the sections we'd expect to see below, but you should add or remove any as needed.*

### Growth of the Business

*What were the biggest changes to the business? How did the customer base change or grow? Did you add new product offerings or enter new markets?*

Over the period [DATE] to [DATE], our customer base grew from [x] to [x]. We launched [x] new products, and entered [x] new markets.

### Growth and Evolution of the Team

*Did you add any new roles this year, i.e. expand your management team or up level the team’s expertise? Did you expand the team’s capabilities, such as building a financial crime focused engineering team or bringing on a team to focus exclusively on QA and training? Has the team been part of a re-organisation to address previous gaps? This is a great chance to highlight how you’ve adapted to changing risks and to call out where there may still be gaps.*

### New Products / Features

*If you’ve launched a number of new products/features this year, it may be worth including a table with a brief description of that product/feature, as well as your assessment of financial crime risk.*

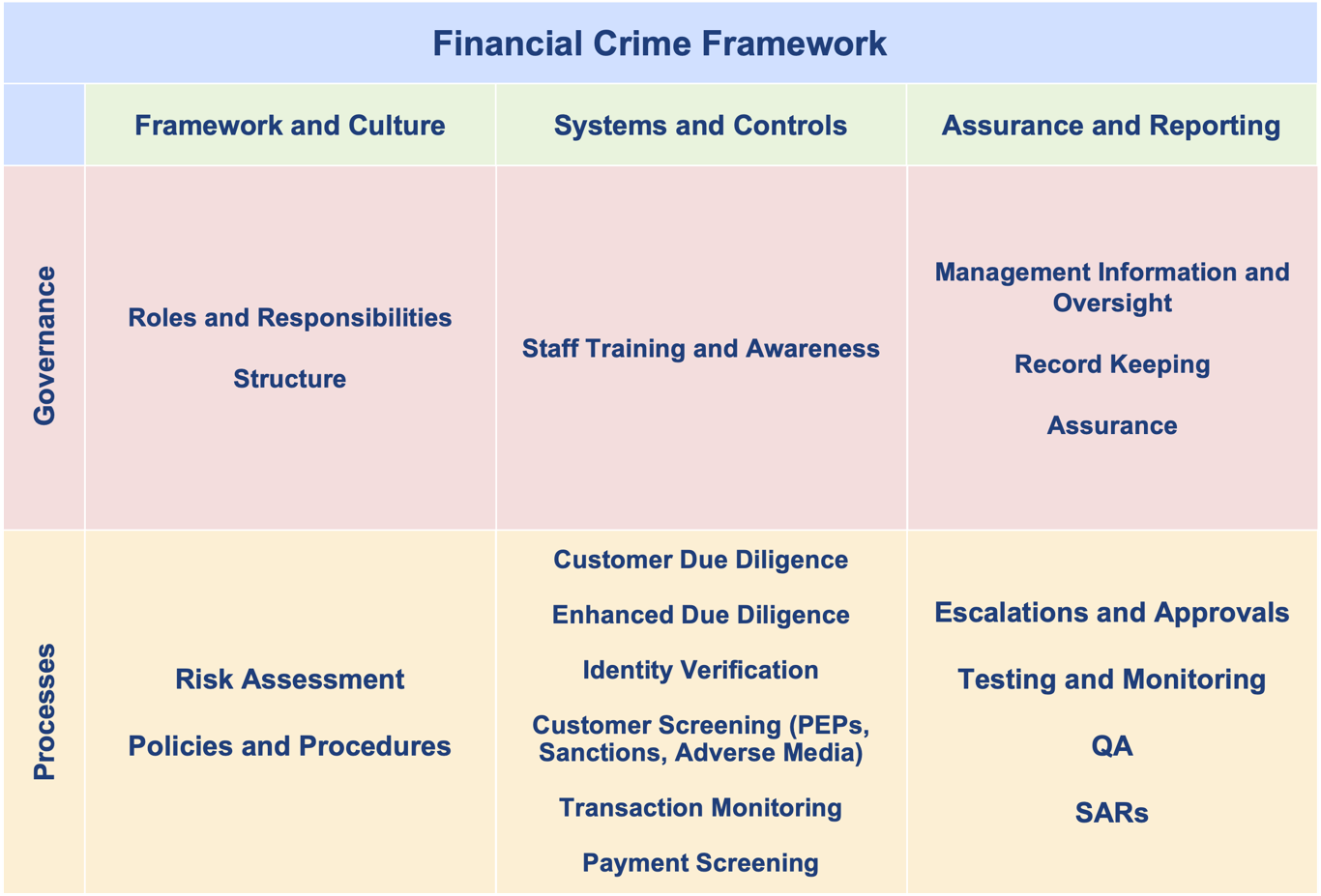
In [YEAR], the company launched [product], which involves higher risk of [money laundering], particularly around [context]. As a result, we’ve [made the following changes]. The financial crime team is also working closely with [team] to ensure money laundering risk is adequately considered prior to the launch [of product / in country].

|  |  |  |  |
| --- | --- | --- | --- |
| **Product** | **Description of Product/Features** | **Key Financial Crime Risk Factors** | **Risk Rating** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Financial Crime Framework

*This section should cover the themes central to your management of financial crime risk, often referred to as areas of the financial crime framework. You likely want to cover the following areas: Governance, Staff Training, Management Information and Oversight, Policies and Procedures, Risk Assessment, Assurance and Regulatory Change, Screening, Customer and Enhanced Due Diligence, Ongoing Monitoring and Reporting.*

Our financial crime framework outlines how we’ve structured financial crime risk management and the key components that make up our strategy.



### AML Governance Framework

*Outline who is responsible for AML systems and controls. You want to make it clear who is responsible for the duties outlined in SYSC 3.2.6I and why they or any delegates are suited for that responsibility.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Name** | **Location** | **Employment Dates** | **Responsibilities** | **Responsibilities Delegated to Others** |
| Chief Risk Officer / Chief Compliance Officer |  |  |  |  |  |
| MLRO |  |  |  |  |  |
| Nominated Officer |  |  |  |  |  |
| *Head of Financial Crime* |  |  |  |  |  |

### Financial Crime Structure

*This is a helpful place to call out how you are utilising your people, processes, systems and governance across the business, especially if you are following the three lines of defence model.*

|  |  |  |
| --- | --- | --- |
| **Line of Defence** | **Teams/Roles** | **Responsibilities** |
| *1st Line of Defence* | *Financial Crime Ops, Financial Crime Engineering, Financial Crime Data Science, Head of Financial Crime* | *Building and implementing controls*  *Managing and conducting financial crime operations* |
| *2nd Line of Defence* | *Compliance, Risk and Controls* | *Financial Crime Assurance programme* |
| *3rd Line of Defence* | *Internal Audit* | *Internal audit - financial crime, enterprise risk* |

### Governance Committee Structure

*Which are the relevant committees that help oversee financial crime governance and what are they responsible for?*

|  |  |  |  |
| --- | --- | --- | --- |
| **Committee** | **Responsibilities** | **Chair / Members by Role** | **Cadence** |
| *Risk and Compliance Committee* | *Identify financial crime risks and issues, ensure appropriate level of oversight and action* | *MLRO, Chief Risk Officer, Head of Financial Crime* | *Monthly* |
| *Executive Committee* |  |  |  |
|  |  |  |  |

### Systems and Control Effectiveness

*This is the body of the report. In this section you want to go through each part of your financial crime framework and talk about what controls are in place and how they have worked over the relevant time period, including the supporting data. We have included the sections we'd expect to see below, but add or remove any as needed.*

### Staff Training

*Training is the first part of your framework and can be a good place to start. We recommend you talk about what training is done, how often, and how it demonstrates your compliance culture. If there are any employees who have not received training in the expected time period, you will want to provide an explanation of why and when this will be completed. You should outline any differences in the training received by the MLRO or other senior staff. It’s also a good place to call out any key milestones and areas of concern if applicable.*

#### Training Completion

All members of staff are required to go through anti-financial crime training at least once a year. Training is prepared by [INSERT] and delivered through/by [INSERT].

Completion rates for the relevant time period were [INSERT].

The MLRO and senior staff consisting of [ROLES] also completed [details of additional training] on [DATE].



In addition to tracking completion, each training includes [quality checks, such as a quiz] to test for awareness.

New joiners of the financial crime team undergo [INSERT amount of time or number of sessions] as part of their onboarding. Members of the financial crime team also go through additional training to refresh their knowledge and stay abreast of any changes. QA findings are used to identify gaps and inform the creation of new training content.

#### Key Milestones

Since rolling out [NEW TRAINING] in [DATE], we’ve seen a [x%] improvement in [decision outcomes].



#### Areas of Concern

*This is a good section to call out any areas of concern or needs around training, for example, needing support from senior leadership in order to build a more robust compliance culture.*

### Management Information (MI)

*In this section it’s important to share key metrics, both to show how effective the programme is as well as to demonstrate how much oversight you actually have. We’ve included suggested sections but you may have others to add or different ways of showing this data.*

*For newer businesses, you may wish to provide more context before diving into the data, so adjust the order of these sections accordingly.*

#### Financial Crime Risk Appetite MI

*The main question you want to address here is: do you know whether or not you’re operating within Risk Appetite? If so, how?*

*This is a great opportunity to include any data you have around your core risk appetite metrics and where you actually stand relative to your threshold. We’ve included three possible examples below: % of customers that are PEPs, % of customers that are high risk, # of SARs per 1000 customers.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Appetite Description** | **Risk Appetite Threshold** | **Was Risk Appetite breached during [YEAR]?** | **Current Level** |
| *% of customers that are PEPs* | *1%* | *Yes/No* | *0.7%* |
| *% of customers that are high risk* |  |  |  |
| *Number of SARs per 1k customers* |  |  |  |

#### Fraud MI

*Do you know how much fraud is going through your systems? How effective are you at stopping it? What visibility do you have around this? This is a great place to highlight the types of fraud you’re seeing or if it’s disproportionately affected any business areas or specific products. Include any details on the narrative, such as how you compare to your peers in the industry. Are you adhering to any industry best practices, such as membership of Cifas or the Contingent Reimbursement Model?*



#### Incidents MI

*How many regulatory or risk appetite breaches or control failures have you experienced this year? How were they dealt with?*



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Title** | **Summary of Incident** | **Occurrence Date** | **Resolution Date** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Senior Management Oversight

*This section provides the opportunity to evidence that the MLRO has the appropriate level of access and authority as required by SYSC 3.2.6I.*

SYSC 3.2.6I requires that the MLRO has a level of authority and independence within the company and access to resources and information sufficient to enable them to carry out their responsibility. The below summarises the primary ways in which they’ve maintained oversight.

* The MLRO has access to key financial crime metrics available via [INSERT]. This is updated in [real time] and contains [INSERT].
* Interface with the [INSERT] teams - [ROLE] attends [MEETINGS] with [TEAMS] on [INSERT] cadence
* Access to external and internal audit and QA findings
* Senior management receives regular reports on [SCOPE]

### Policies and Procedures

*When was your financial crime policy last updated? Is it still fit for purpose? Is it adequate and effective to meet legal and regulatory requirements? What key policy changes have been made? Does it account for upcoming regulatory changes? Does it cover all areas of the business? Do your policy and procedures cover the following areas: Due Diligence, Risk Assessment, Training, Record Keeping, SARs, Ongoing Monitoring, and Sanctions Screening? Have any new systems, processes and products been incorporated? This is also a good opportunity to call out how you use the JMLSG Guidance, FCA guidance, or any other sources.*

Policies and procedures are critical to the effective management of our financial crime risks and it’s the [COMPANY’s] responsibility to ensure they are adequate, up to date and effectively embedded across the business. Our Financial Crime Policy was last approved at [Board] on [DATE].

#### Key Milestones

Our policies covering the areas [INSERT] have been updated in [YEAR] to account for [regulatory change, new products, maturity, business expansion, etc].

Our procedures on [list] were reviewed during [date range] and updated to reduce the risk of manual errors. However, [riskiest procedures] remain areas of high risk due to the [manual nature of the procedure].

All policies and procedures have been reviewed and approved by the MLRO as of [DATE].

#### Areas of Concern

*This is a good section to call out any areas of concern - i.e. have you identified any gaps in documented procedures or guidance to staff? Any outdated content that drove incorrect outcomes? Any reasons to doubt compliance with the regulatory requirement to have adequate policies and procedures?*

### Risk Assessment

*SYSC 6.3.3R requires that a “firm 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”. This section is an opportunity to demonstrate that you have a risk assessment in place and it’s fit for purpose, as well as when it was last updated and how it’s maintained. How have your risks evolved in the last year? What are your top 3 risks? How are these risks and their mitigants documented? How does this risk vary across products? Across countries?*

Our financial crime risk assessment should ensure that all financial crime risks to the business are identified and documented so that we can ensure our systems and controls are comprehensive and proportionate to the growth and maturity of the business. Our risk assessment was implemented in [DATE] and is reviewed by [committee/owner] on a [cadence] basis.

Throughout [YEAR], our primary financial crime risks have [increased / remained stable / decreased] due to [factors]. Our top three current risks are [list]. Our risk assessment has evolved to include [changes] which have allowed us to better track and monitor our risk exposure.

#### Key Milestones

*Any major changes to your risk assessment? Did you identify new risks or see a significant shift in your risk profile?*

Our risk assessments for [business areas] have been updated in [YEAR] to account for [change] and were reviewed and approved on [DATE].

#### Areas of Concern

*This is a good section to call out any areas of concern - i.e. have you identified any gaps in documented procedures or guidance to staff? Any outdated content that drove incorrect outcomes? Any reasons to doubt compliance with the regulatory requirement to have adequate policies and procedures?*

### Assurance

*You may wish to provide more context about your structure - how many people make up the 2nd and 3rd lines, and what cadence/form does assurance take? For example, do you have monthly assurance meetings for each business area, a risk assessment that’s been reviewed/agreed, monitoring programmes, etc. How do you know these have been impactful?*

There are [INSERT] full time employees in the [INSERT teams] dedicated to financial crime oversight and assurance. They conduct [INSERT] meetings on [cadence], in order to [purpose]. In [YEAR] they implemented [programmes, process, etc], which [had this impact].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Business Area 1** | **Business Area 2** | **Business Area 3** | **Business Area 4** |
| *Risk Assessment* | *Implemented [DATE]* | *Implemented [DATE]* | *Implemented [DATE]* | *Implemented [DATE]* |
| *Assurance Meetings* | *Monthly* | *Quarterly* | *None* | *Weekly* |
| *2LOD Monitoring Programme* | *10% of auto approved accounts manually reviewed*  *100% of offboarded accounts manually reviewed* | *1% of accounts manually reviewed* | *Ad hoc reviews only* | *Ad hoc reviews only* |
| *Management Information* | *Assurance MI is readily available and reviewed by governance committee* | *Effectiveness metrics are available and reviewed quarterly* |  |  |

The 2LOD Assurance Programme is composed of [INSERT] main components: [INSERT - i.e. manual dip sampling, monitoring of MI, routine assurance reviews, etc].

The 3LOD conducts an internal audit every [CADENCE] which includes the financial crime programme. Their findings and recommended actions are tracked [INSERT] and owners are assigned from [INSERT, i.e. 1LOD and 2LOD].

#### Key Milestones

*This may be a good opportunity to share key pieces of assurance work. Have you responded to assurance findings from previous reports? How do you conduct quality assurance? Who is responsible for this, what specific controls/processes are QA’d, what is your sampling methodology, and what are the key findings and projects?*

[x%] of [Transaction Monitoring] tasks are reviewed for quality assurance. The primary areas tested are: [appropriateness of flag, accuracy of decision, adherence to policy and procedure].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Breaches or Failures Identified via Assurance** | **Type of Finding** | **Outcome** | **Owner** | **Due Date** |
| *Previous rules are no longer performing well due to growth - increase in flags and decrease in TPs* | *Control failure / regulatory or risk appetite breach / control gap / inadequate or ineffective controls* | *Risk accepted / root cause fixed / in progress* |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### Areas of Concern

*How confident are you that your assurance programme is adequate and effective? Are there any gaps worth calling out? When you do identify issues, do you have the resources to fix them, or even size them?*

### Overview of [INSERT Business Area - i.e., business banking, merchant services, crypto wallet]

*This is an opportunity to share the overall narrative around a specific business area. How has the area changed or grown this year? What controls do you have in place for each area of your financial crime framework, and how effective are they? What issues have you identified and how have you dealt with them?*

*You can copy/paste section 7 for each business area.*

### Growth / KPIs

*What has the growth been like? How has your customer base changed? What are your overall KPIs?*

### Summary of Controls

*Provide a high level overview of performance across your financial crime controls: what areas are working well? What areas are you most concerned about? We’d expect to see updates on at least the following areas: PEP/Sanction screening, IDV, customer risk assessment, transaction monitoring, reporting.*

* Overall, our [INSERT controls] were effective at detecting and deterring [INSERT risks].
* Our [INSERT control/process] improved [INSERT %] after [INSERT actions].

### Key Milestones and Areas of Concern

*Were there major changes to the team this year, and what impact did they have? What about changes to your controls or tooling? Were you required to change how you think about prioritisation or implement externally required changes (such as confirmation of payee or 3DS 2.0)?*

*This is a good place to call out the largest problems seen this year: what are the main challenges you faced? What about incidents?*

### Onboarding Controls

*What key controls do you have in place at onboarding? How do you know they’re working? It may be helpful to show a diagram of your controls and where they come into play throughout the life cycle of an account so we’ve included an editable example below. You may also want to show some statistics in the diagram, to indicate how many flags and true positives are identified at each stage.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Onboarding Controls** | **KYC Checks**  # auto approved:  # manually approved:  # auto rejected:  # manually rejected: | **Identity Verification Screening**  # auto approved:  # manually approved:  # auto rejected:  # manually rejected: | **Adverse Media Screening**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: | **PEP Screening**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: | **Sanctions Screening**  # flagged:  # false positive:  # true positive rejected: | **Cifas Checks**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: | **[Other Fraud Checks]**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: |
| **Customer Risk Assessment**  # outside of risk appetite:  # high risk:  # medium risk:  # low risk: | | | | | | |
| **Enhanced Onboarding Controls** | **Enhanced Due Diligence**  # flagged:  # auto approved:  # manually approved:  # auto rejected:  # manually rejected: | | **Source of Wealth**  # requested:  # received:  # accepted:  # rejected: | | **Source of Funds**  # requested:  # received:  # accepted:  # rejected: | | |
| **Ongoing Monitoring** | **Transaction Monitoring**  # flagged:  % false positive:  % true positive no action:  % true positive SAR’d:  % true positive exited: | | **Ongoing PEP Screening**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: | | **Ongoing Adverse Media Screening**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: | | **Ongoing Sanctions Screening**  # flagged:  # false positive:  # true positive accepted:  # true positive rejected: |
| **Outcomes** | **Suspicious Activity Reports**  # SARs from TM:  # SARs identified internally:  # SARs identified externally: | | **OFSI Reports**  # OFSI Reports:  % OFSI Reports identified internally:  % OFSI Reports identified externally: | | **Outside of Risk Appetite**  # accounts exited outside of risk appetite:  # accounts exited identified internally:  # accounts exited identified externally: | | |

At onboarding, [x%] of attempted signups are typically rejected, which we believe reduces the number of bad actors using our services. A customer risk rating is assigned at onboarding which dictates whether an account can be automatically approved or requires more information for them to [complete signup or begin transacting].



The below graph is an estimation of our onboarding control effectiveness based on our dip sampling of accounts.



### Effectiveness of Screening

*It may be helpful to provide a brief summary of your approach to screening (i.e. vendors used), any impactful changes and generally whether it’s been adequate and effective. If you utilise Adverse Media checks, you may wish to add an additional subsection.*

Since [DATE], we have used [VENDOR] to conduct PEP and Sanctions screening. We have used [VENDOR] for identity verification checks since [DATE].

#### Politically Exposed Persons Screening

*This is a good section to discuss your requirements around PEP screening and to highlight any impactful changes and whether this control has been adequate and effective.*

We are required to apply a risk-based approach to identifying Politically Exposed Persons (PEPs), and to apply a risk-based approach to performing enhanced due diligence on any PEPs. All true positive PEPs must be approved by [ROLE] prior to account opening and their risk rating must take their PEP status into account. This ensures that an appropriate level of due diligence is applied. Checks are conducted as part of onboarding as well as ongoing checks every [CADENCE].



*You may wish to explain that PEPs themselves have different risk levels, by showing the split of risk ratings across PEPs.*



*You may wish to show the operational effectiveness of this screening, such as how many flags are raised each month and the true positive rate. We’ve included an example below.*



#### Sanctions Screening

*This is a good section to discuss your requirements around Sanctions screening and your approach, such as which lists are used, the frequency of checks and the types of entities/payments that are screened. You should also highlight any impactful changes and whether this control has been adequate and effective.*

Sanctions screening checks are conducted as part of onboarding as well as ongoing checks every [CADENCE].

*You may wish to include some statistics showing the operational impact and effectiveness of this screening, such as how many flags are raised each month.*



*You may also wish to evidence how you’ve handled any true positive sanctions hits.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date Discovered** | **Had Transacted?** | **Date Reported to OFSI** | **Date Response Received from OFSI** | **Date Customer Offboarded** |
|  | *Yes/No* |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### Identity Verification Checks

*This is a good section to discuss your requirements around identity verification and to highlight any impactful changes and whether this control/process has been adequate and effective.*

Checks are conducted as a part of onboarding. Any failed or unclear results from the vendor are manually reviewed.

*You may wish to include some statistics showing the impact and effectiveness of this screening, such as the split of IDV outcomes. We’ve included an example below.*



#### Vendor Effectiveness

*This is a good opportunity to share conclusions about how confident you are in your vendors’ effectiveness. You may wish to include some statistics showing the overall effectiveness of your screening, based on your testing and assurance. We’ve included a sample graph below.*

The below graph is an estimation of our effectiveness based on our dip sampling of accounts. We review [x%] of accounts every [cadence].



### Effectiveness of Customer Risk Rating

*This is a good section to discuss your requirements around customer risk assessments and to highlight any impactful changes and generally whether this control/process has been adequate and effective.*

[INSERT] % of customers are assigned a risk rating at signup via [process]. The risk rating impacts the [onboarding flow] and the cadence for [ongoing reviews]. Risk ratings can be adjusted by [INSERT - manual review vs auto only, etc].



*You may wish to show the overall split across your customer base by risk rating, as well as contextualise any spikes or shifts. For example, did you make a change to how you assess risk rating, which resulted in a number of low customers being re-classified as medium risk?*



*This is also a good opportunity for you to show how effective your risk rating is. For example, if you look at customers you ended up SARing, how accurate was their initial risk rating? We’ve included a suggested graph below.*



### Effectiveness of Customer and Enhanced Due Diligence

*This is a good section to discuss your requirements and to describe what due diligence you apply at the time of application and on a risk-based approach. What key controls do you have in place and how do you know they’re working? You should also highlight any impactful changes and generally whether this control/process has been adequate and effective.*

Customer Due Diligence (CDD) includes all the details we require at onboarding or prior to a customer being able to transact. Our onboarding controls ensure that we remain compliant with JMLSG best practices.

The below graph is an estimation of our onboarding control effectiveness based on our dip sampling of accounts.



Enhanced Due Diligence (EDD) is applied to any customer with [a high risk rating] or as part of our ongoing monitoring.

### Financial Inclusion

*SYSC 6.3.7G requires that our systems and controls include “appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity”. Use this section to describe any exceptions to your policies for the purpose of financial inclusion, such as your customer identification policy. You should also outline your process for dealing with customers who are, or may be, financially excluded.*

SYSC 6.3.7G requires that our systems and controls include measures to ensure fair treatment of customers who may be financially excluded. As a result, we have specific exceptions to our [INSERT process or control] which allows us to offer accounts to customers who may not be reasonably able to provide the evidence of identity we typically require.

### Effectiveness of Ongoing Monitoring

*The FCA requires that firms “must conduct ongoing monitoring of its business relationships on a*

*risk-sensitive basis.” It may be helpful to provide a brief summary of your approach to ongoing monitoring - what key controls do you have in place and how do you know they’re working? You may also wish to include the following subsections.*

#### Source of Funds and Source of Wealth

*Firms are required to “take adequate measures to establish the source of wealth and source of funds” for individuals identified as PEPs or close associates. In this section you should explain when and how you carry out Source of Funds and Source of Wealth checks, for example when carrying out EDD for PEPs or for particularly unusual activity. You should also mention the outcomes of those Source of Funds or Source of Wealth checks.*

We carry out Source of Funds and Source of Wealth checks for all [INSERT criteria].

#### Transaction Monitoring

*Are your transaction monitoring processes adequate and effective? Have you introduced any new rules or vendors? Are you able to review risky transactions in real time or do you have significant operational backlogs? Is your transaction monitoring system in the authorisation loop i.e. can you stop suspicious funds from leaving an account, or is the system retrospective?*



*This may also be a good section for you to share your rule catalogue if you have one - it’s a great chance to evidence how the controls you have relate to specific financial crime risks.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of Rule** | **Description of Rule** | **Crime Type or Risk targeted** | **Total Flags in [time period]** | **True Positive Rate** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*This is also a good opportunity for you to show how effective your transaction monitoring is at detecting financial crime. For example, if you look at the total financial crime you’re aware of, what percentage did your transaction monitoring rules actually flag? We’ve included a suggested graph below.*



#### Law Enforcement and Other External Intelligence

*Are you meeting your legal requirements around responding to law enforcement requests? How has your engagement with law enforcement and other external intelligence agencies or banks evolved this year? Are you a member of JMLIT or any other industry bodies? Are there any trends worth highlighting or any areas of concern around your process for external communications?*

We received [number] of reports from law enforcement and other external sources in [YEAR]. The majority of requests related to [crime types].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Crime Type** | **Number of Reports** | **Number Resolved / Outstanding** | **Recommended Actions** |
| *Law Enforcement / Bank / Other* | *Fraud / Money Laundering / Terrorist Financing* |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

We were compliant in our response to [x%] of court orders.

|  |  |  |  |
| --- | --- | --- | --- |
| **Court Orders Received** | **# Responded within Deadline** | **Nature of Court Order** | **Recommended Actions** |
| *Law Enforcement / Bank / Other* | *Fraud / Money Laundering / Terrorist Financing* |  |  |
|  |  |  |  |
|  |  |  |  |

### Suspicious Activity Reporting

*This is a good section to describe the types of crime you’ve identified and how this has impacted your understanding of your risk profile. It’s also an opportunity to highlight any peer comparisons if publicly available. Were there any significant trends that might indicate the need for changes, i.e. to your risk appetite, transaction monitoring rules, staff training, etc?*



In [YEAR], we submitted [x] SARs that identified [INSERT crime types].

