FIAU
Financial Intelligence Analysis Unit
Malta

Corrective Actions Paper

June 2025

Table Of Contents

Table of Contents

1. Introduction

Subject Persons (SPs) must maintain strong control frameworks to ensure compliance with anti-money laundering (AML) and combatting the financing of terrorism (CFT) obligations, especially as criminals increasingly attempt to exploit and misuse the financial system. The core of The Financial Intelligence Analysis Unit's (FIAU) mission is to ensure compliance with AML/CFT legislation, including ensuring that robust controls are in place to safeguard the integrity and reputation of our financial system. A way to ensure that the FIAU is effective is through imposing Directives requiring corrective actions to be taken by SPs. These administrative measures are aimed at restoring compliance with the applicable AML/CFT legislation.

The purpose of Directives are to enhance SPs' AML/CFT compliance frameworks and ensure they are better equipped to swiftly detect potential money laundering and/or financing of terrorism (ML/FT) and take the required action in line with the relevant AML/CFT Regulations. Additionally, Directives also provide for an additional communication platform between SPs and the FIAU, creating a space for representatives of the SPs to discuss AML/CFT issues and matters they face directly with representatives of the FIAU, thus uniting efforts towards combatting ML/FT.

Through this paper we aim to expand on the administrative measures imposed by the FIAU that are aimed at ensuring the necessary corrective actions are taken. This paper also provides an explanation of the different types of Directives which may be imposed and the enforcement process behind the FIAU's monitoring of SPs' adherence to the Directives. Furthermore, it provides statistics covering several aspects of Directives (inc. meetings held, type of AML/CFT matters discussed and the outcomes of the Directives), notable good practices, areas which require improvement and key takeaways are also covered within this paper.

This paper is to be read in conjunction with other guidance notes and papers which were issued by the FIAU in previous years, including the Enforcement Factsheet[1] issued in January 2024 which serves as a foundation for this paper, given that the corrective actions process is a continuation of the process covered in the previously published Factsheet.

[1] https://fiaumalta.org/app/uploads/2024/01/Enforcement-Factsheet-A-Compilation-of-Regulatory-Actions-20212022.pdf

2. Ensuring Tangible and Effective Corrective Actions

2.1 The Enforcement Process Leading to the Imposition of Directives

During the enforcement process,[2] the Compliance Monitoring Committee (the CMC or the Committee) determines the administrative measures to be imposed on SPs for breaches of AML/CFT obligations, including the potential imposition of an administrative penalty. However, it is imperative to note that the Committee's aim is to restore and/or enhance compliance, therefore a Directive aimed at taking corrective actions is customary when breaches are determined.

2.2 Directives Aimed at Ensuring Corrective Actions

In imposing a Directive to take remedial actions, the Committee will consider the systematic nature of the breaches as well as its materiality, and on this basis it will issue a Directive that reflects the same. The intrusiveness and intensity of its measures will equally be directed on these same considerations, thereby ensuring a risk-based application of directives.

The Committee will impose one of the following Directive types, starting from the least stringent:

1. Remediation Directive (including the possibility to opt for written declarations)
2. Follow-Up Directives

2.2.1 Remediation Directive

This form of Directive is the least stringent and, in some cases, may only require the SP to provide a declaration of compliance confirming the remedial action that has been undertaken. It is imposed in circumstances where the Committee believes that there is no need for the enforcement officials to be thoroughly involved in the SP's remediation. This happens when the breaches are not of significant materiality and/or the representations submitted by the SP focus on the remedial action already undertaken or the planned actions for which the Committee is satisfied with the evidence at hand.

SPs are given between three to nine months to respond to the requests made by the FIAU, or to explain why the remedial measures required cannot be implemented within the set timeframes. Remediation Directives typically request the updating of policies and procedures, together with their implementation. Upon receipt of the information/documentation, the enforcement Section reviews its contents and, if necessary, requests further information and/or documentation demonstrating the SP's compliance with the issued Directive.

[2] For more information on the Enforcement process, please refer to the Enforcement Factsheet published in January 2024 (page 4), which outlines the procedure followed by the Committee.

Meetings may also be held to provide a live demonstration of the systems implemented (where applicable) or to clarify additional matters as may be required. A small sample of files may also be reviewed to assess the SPs remediation in practice; however, this is done on a case-by-case basis and depending on the outcome of Phase 1 as detailed in Section 2.3.

Between 2020 and 2024, the FIAU imposed 60 Remediation Directives, additional statistical breakdown per sector and case studies pertaining to Remediation Directives can be found under Annex 1 and 2 of this paper.

2.2.2 Follow-Up Directive

A Follow Up Directive is the most intrusive form of Directive the Committee may impose. This is selected when the Committee believes that the FIAU's enforcement section should have oversight to initiate or facilitate change or improvement in a subject person's AML/CFT control framework or specific aspects of it. When a Follow-Up Directive is imposed, the SP is expected to submit an Action Plan with clear action points highlighting the remedial actions planned in relation to the identified breaches, together with the respective task owners and target dates for completion. Periodic meetings are held with the SP to assess the level of remediation undertaken. These are followed up by multiple requests for information/documentation to prove implementation. Furthermore, system walkthroughs (where applicable) and file testing are conducted as part of the Follow-up Directive, to prove the effective implementation of the Action Plan and to ensure that the action points were completed.

Between 2020 and 2024, the FIAU imposed 41 Follow Up Directives, additional statistical breakdown per sector and case studies of Follow-Up Directives can be found under Annex 1 of this paper.

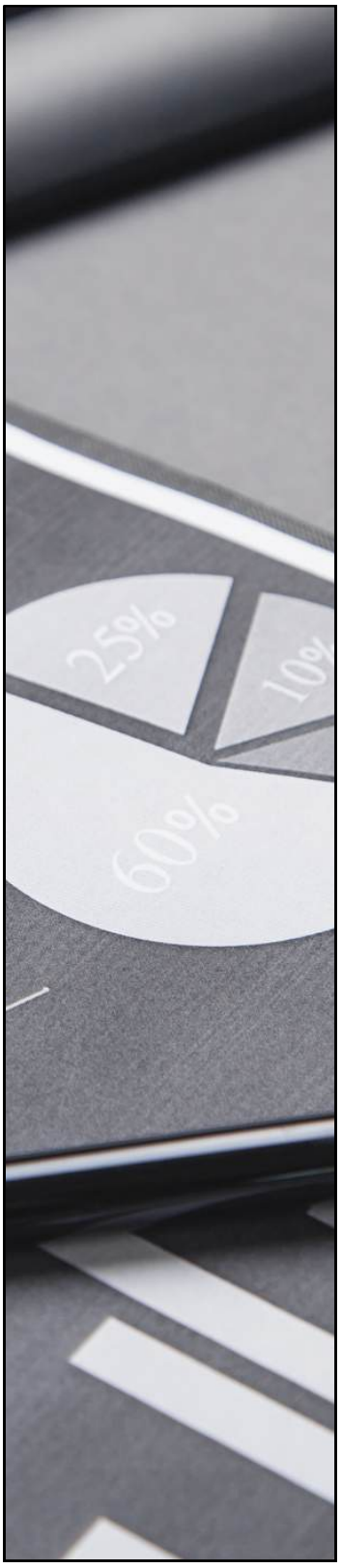
Table 1 illustrates the main differences between the two types of Directives, i.e. Remediation and Follow Up Directive.

Remediation Directive	Follow Up Directive
3 – 9 months to adhere to FIAU's request	Up to 10 weeks to provide Action Plan
No Action Plan Required	Action Plan and timeframes for completion are endorsed by the FIAU
One off Meetings	Frequent meetings between FIAU and SP
Minimal requests for information/ documentation	Multiple requests for information/ documentation
Requests for clarifications (if required)	Multiple requests for clarifications
Small sample of files (if required)	Sample of files

Table 1: Differences between Remediation & Follow Up Directives

2.3 The Two-Phased Process Logic of Directives

Both the Follow-Up and Remediation Directives have a two-phased process to ensure that all reviews are conducted in a risk-based manner. Phase One encompasses the assessment of the Technical Compliance and Design of the AML/CFT controls in areas that were deemed inadequate during the examination. Phase Two tests the effectiveness of such controls. As a result, the outcome of Phase One directly impacts the extent of testing in Phase Two.



2.3.1 Phase One – Technical Compliance and Design

This phase includes the testing of the adequacy of the SPs remediation insofar as the technical compliance and design of their AML/CFT framework is concerned. The Corrective Actions Team within the enforcement section of the FIAU conducts validation on the following areas:

A. Action Plan:

The submission of an Action Plan is a requirement for SPs that have been served with a Follow-Up Directive. Aside from ensuring its timely submission (as indicated in the Administrative Measures Letter), Enforcement Officials ensure that the Action Plan includes:

- Planned/completed remedial actions on **all breaches** of AML/CFT outlined in the issued Administrative Measures Letter and imposed under the Directive.
- **Clear and concise** descriptions of the planned/completed remedial actions.
- **Set timelines**, specifying the date of completion/expected completion of each action.
- Reference to the SP's **representative leading** the respective action point.
- Reference to any **supporting documentation** provided/to be provided, demonstrating the work completed regarding each action.

Any divergence between the submitted Action Plan and the FIAUs requirements must be addressed by the SP until the plan is deemed acceptable and endorsed by the FIAU. If these divergences remain unresolved, the matter will be referred to the CMC for any action it considers appropriate.

B. Policies and Procedures:

This includes an assessment on the SPs' written policies and procedures. Depending on the actions necessary as part of the Directive imposed, the following documents are usually requested from the SP and are reviewed by the FIAU:

- AML/CFT Policies and Procedures (including Customer Acceptance Policy)
- Business Risk Assessment
- Customer Risk Assessment Methodology
- Onboarding Forms
- Ongoing Monitoring Forms
- Transaction Monitoring Policies
- Alerts Handling and Management Procedures
- Internal SAR/STR Policies and Forms.

As part of the assessment, SPs may be required to clarify specific aspects of their implemented processes or procedures and to demonstrate alignment with the actual controls in place.

C. System Walkthroughs:

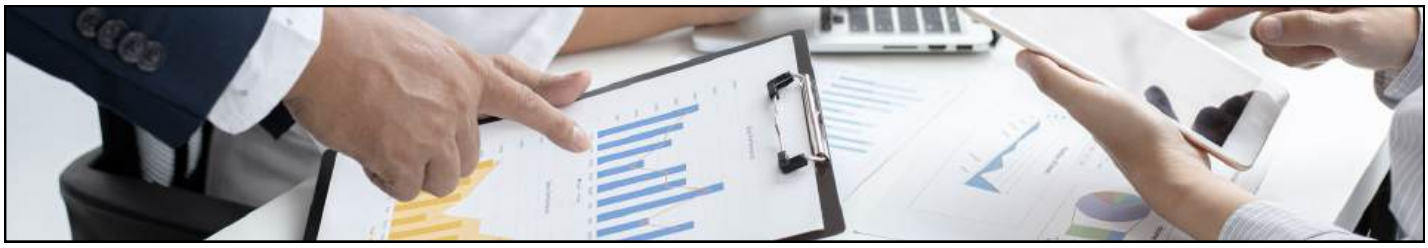
To demonstrate the SPs implementation of its policies and procedures, SPs may be required to provide system walkthroughs to showcase integration with its internal systems and tools. This helps validate the systems' ability to identify, assess, and monitor risks appropriately. Additionally, these walkthroughs also serve to understand how systems are working and communicating together to enhance the SPs operations.

System Walkthrough Example: SPs may be asked to conduct a live walkthrough showcasing their understanding of how the different risk profiles are being assessed, monitored, and reviewed in practise. This may also include obtaining an understanding on the handling of transaction monitoring alerts, adverse media and alerts in relation to profile changes.

System walkthroughs may be requested in instances where an SP makes use of the following:

- Compliance Management Systems
- Customer Risk Assessment Tools
- Customer Onboarding Systems
- Ongoing Monitoring Tools and Screening Systems

The assessment on technical compliance and design enables the Corrective Actions Team to understand the effectiveness of these controls, if implemented correctly. When the Remediation Directives assessed during this phase are deemed inconclusive or exhibit deficiencies in the technical compliance or design of the control framework, they proceed to the second phase: control effectiveness testing. Since Follow-Up Directives inherently include an element of effectiveness testing, they automatically proceed to the second phase.



2.3.2 Phase Two – Control Effectiveness Testing

Phase Two considers two factors:

1. The type of Directive imposed, i.e. whether a Follow-Up Directive or a Remediation Directive was imposed.
2. The outcome of Phase One.

These two factors are considered when deciding the extent to which the effectiveness of the remediated controls are tested while ensuring that the assessment is risk-based. This specifically impacts:

- Whether to request a sample of customers for review.
- The extent of customer data requested for sample selection (if applicable).
- The size of the customer sample (if applicable).

The following is a non-exhaustive list of documentation that may be requested upon selection of the customer files chosen for review:

- Onboarding forms
- Customer Risk Assessment carried out (at onboarding and after)
- Customer due diligence collected (at onboarding and after)
- Ongoing monitoring forms
- Documentation collected as part of the ongoing monitoring carried out
- Transaction history or bank statements
- Transaction monitoring reports including any alerts generated, and any supporting documentation collected as part of the transaction monitoring review or alerts handling process
- Correspondence with the customer.

Further clarifications may be requested, particularly where the tangible progress expected from the corrective actions undertaken cannot be evidenced.

2.3.3 Meetings with SPs

During either phase of the Directive, enforcement officials may deem it necessary to request a meeting with representatives of the SP. Meetings are generally requested when:

- System walkthroughs or demonstrations are required.
- Clarifications are necessary.
- The SP's knowledge is to be proven.
- About other relevant matters as deemed appropriate.

If a meeting is required, an agenda is circulated to the SP to ensure enough time is provided to prepare and ensure the right resources are available.

Between 2020 and 2024, 262 matters were discussed during **151 Directive meetings** held between the Corrective Actions Team and SPs. Annex 1 provides further details on the topics discussed during Directive meetings.

2.3.4 Conclusion of Directives

The Corrective Actions Team presents the case to the CMC after the testing phase/s. The CMC is given a detailed breakdown by the Team to show if tangible progress has been made by the SP on the remediation, whether areas for improvement are still outstanding, or whether little to no progress has been registered. The Committee then deliberates on whether to close the Directive or to mandate additional corrective measures, and the following decisions may be taken by the CMC:

**The table is available overleaf*

In the event of successful remediation

A closure letter stating this is issued to the SP, closing the directive without further comments or recommendations.

Where further improvements are required

The CMC may issue a closure letter with recommendations or expectations to remediate further.

Failure to carry out required remediation

Where the Committee determines that keeping a Directive active has no further value yet remains unsatisfied with the SP's progress, it may issue a closure letter with reservations. These reservations indicate that the Committee is unable to confirm the effective implementation of the remedial actions undertaken.

This outcome is communicated to the FIAU's Supervision team, enabling them to monitor the implementation of the relevant controls during future supervisory engagements.

In these cases, the prudential regulator may also be informed that the Committee was not satisfied with the remediation efforts. This notification typically includes details of the Committee's concerns for the prudential regulator's consideration.

Where the Committee believes that the risks have not been adequately managed and remain predominantly exposed, it may impose further administrative measures, including either the imposition of an administrative penalty for breach of the Directive imposed or a daily pecuniary penalty until compliance is restored and/or enhanced.

3. Expectations During Remediation and Follow-up Directives

This section provides SPs with more insights into what to expect during the Directive process. It covers requests for information, meetings, feedback, escalation and closure. In this section, SPs will also be provided with pointers to keep in mind when going through a remediation or follow-up process with the FIAU.

3.1 Collaboration and Cooperation

Directives requiring corrective actions aim to ensure that SPs implement effective controls, to comply with legal obligations, protect their operations and the wider jurisdiction from money laundering and terrorist financing (ML/FT) risks.

Active cooperation with the Corrective Actions Team is essential to ensure the process is thorough, efficient, and effective.

Cooperation between all parties ensures that accurate information can be gathered. This leads to a clearer assessment of policies, processes and systems. It not only improves the efficiency of the process itself but also ensures transparency, demonstrating a commitment to enhancing one's internal AML/CFT controls. Furthermore, cooperation during this process helps identify areas for improvement, enabling constructive feedback, which will ultimately lead to implementing sustainable and effective controls.

Collaboration is core to effectively implementing the actionable points in a Directive. Ultimately, the purpose of a Directive is not to assess past compliance, but to ensure that future compliance is attained and that this is sustainable and long-term. Therefore, the SP and the Corrective Actions Team collaborate closely to achieve this. Providing clear information and highlighting challenges and difficulties encountered during the process ensures that joint efforts by both parties will lead to the desired effective outcomes.

Most SPs undertaking a Remediation or Follow Up Directive have been extremely cooperative and collaborative during the process. This included meeting established deadlines, submitting complete information and documentation, and being available when necessary. A fair number of SPs also request additional meetings on their own initiative, highlighting either other remedial measures outside the scope of the Directive or otherwise to discuss upcoming projects to strengthen their AML/CFT controls. On the other hand, failing to cooperate may adversely affect the outcome of the Directive, particularly when the SP is not cooperating due to negligence or disregard.

Do's	Don'ts
Be responsive.	Consistently be unavailable for meetings.
Ensure sufficient resources are dedicated to the implementation of all actionable items.	Fail to respond to meeting requests or neglect providing the requested information/ documentation.
Keep the management body/board informed of updates related to the Directive (where applicable).	Provide ambiguous replies to questions.
Be available for meetings and make topic-appropriate personnel available.	Be evasive on providing updates related to pre-set targets as set in the Action Plan.

3.2 Supporting Documentation

Supporting documentation showing the actions taken by SPs to address identified failures and strengthen controls is essential to both Follow-Up and Remediation Directives. Documentation shows the SPs' commitment to an effective AML/CFT control framework. Documentation forms the basis of the assessment undertaken by the Corrective Actions Team to verify the remedial action undertaken, as part of phases one and two of the Directive process.

Therefore, it is important to highlight the significance of submitting well-structured, comprehensive, and relevant supporting documentation. This facilitates the smooth progression of the Directive process and reflects the level of commitment demonstrated by the SP in showcasing the appropriate remedial actions.

Do's	Don'ts
Be clear when the necessary changes have not yet been implemented and provide justified timeframes for implementation.	Provide immaterial or cosmetic changes to the previously held policies and procedures which were inadequate.
Highlight planned changes and provide evidence only when the updates have been concluded.	Provide inconclusive policies and procedures without a clear timeframe for conclusion and approval.
Provide evidence of internal testing or independent audit assessments highlighting consistent application of policies and procedures.	Provide documentation that allows for a process that significantly diverges from the one explained during meetings.
Be concise and clearly label the documentation with the actionable item it addresses.	Provide unnecessary documentation without explaining the link with the action undertaken or the reason for submission.
Answer clearly and be transparent about the non-provision of documentation or information, providing a rationale.	Provide selective information and evasive clarifications to queries raised by the Corrective Actions Team.
	Provide only generic statements or documents when demonstrating how the customer profile was established and showcasing the monitoring undertaken.

3.3 Deadlines and Timeframes

Directives target future compliance, which should be achieved in the shortest possible timeframe, avoiding unnecessary exposure to ML/FT risks that would not be effectively managed and mitigated. Therefore, SPs must come up with realistic timeframes to ensure that they can implement effective controls and adhere to the implementation timeframes.

It is understood that certain actionable items, such as implementing systems and measures, may depend on external parties and take longer than expected. However, SPs are still encouraged to factor this in as much as possible when establishing the timeframes for implementation. Also, SPs should ensure that the implementation of the progress made is thoroughly monitored and material divergences from expected timeframes are immediately communicated to the Corrective Actions Team.

Over the years, the majority of SPs have complied with the Directive and the agreed timeframes. It was also encouraging to observe that in the few instances where SPs were not going to adhere to the agreed deadlines, they had promptly informed the Corrective Actions Team and provided the reason for delay, along with proposals for new deadlines.

Do's	Don'ts
Commit to realistic timeframes that will enable the necessary development, implementation, and testing to be carried out, while proving that the corrective action will be efficiently executed.	Commit to extremely tight and unrealistic deadlines. These do not impress or show exceptional commitment to AML/CFT controls. Rather, they will lead to different problems when the deadlines are missed.
Explain the timeframe allocated to each milestone to develop a particular actionable item.	Provide action plans without timeframes or with timeframes that are too wide.
Provide timely updates on implementation and highlight any challenges foreseen.	Inform the Corrective Actions Team that a deadline will not be met only when nearing the pre-established deadline.
Communicate any potential risk of a missed deadline and provide a plan to remediate as soon as possible.	Take a lax approach in monitoring the progress of each action item.

3.4 Further Recommended Actions

Additional areas for improvement may be observed during a Directive or as part of its closure. The implementation of these additional recommendations do not need to be monitored by the Corrective Actions Team, however the SP is expected to take the recommendations onboard and implement them. The FIAU reserves the right to confirm or revisit the recommendations made during a later compliance review as part of its supervisory process.

The below are common recommendations made to SPs by the FIAU as part of the Directive process:

Risk Understanding
Ensure that an explanation of how a control is assessed can be provided.
Ensure that a rationale behind the determination of the level to which controls are deemed effective is retained and can be explained.
The National Risk Assessment (NRA) and Supranational Risk Assessment (SNRA) contain information that will shape the SP's understanding of their risks. One is expected to ensure that the threats and vulnerabilities identified in the NRA and SNRA, which may impact one's operations, are effectively considered and assessed.
SPs cannot rely on a one-size-fits-all, tick-box approach to understand the risks at the business and customer levels. It is essential to ensure that risk factors are tailored to the organisation's specific exposures and assessed in alignment with its business operations, with the prerequisite that any proposed controls have already been implemented.
Risk understanding is best achieved when considering historical information. Therefore, SPs who have been operating for several years and servicing customers for years should ensure that this historical information is leveraged to understand risks and ensure that controls are geared up to manage such risks.
SPs must ensure that manual interventions or subsequent adjustments to a customer's risk assessment are well documented, and the reason is clear and justifiable. Equally, SPs are to ensure that if manual interventions are the rule rather than the exception, and therefore there is a high incidence of manual override, the CRA must be recalibrated to adequately capture risks more effectively.
With a robust risk assessment, SPs can ensure that potential red flags or risk triggers are gauged and that the SP can direct its resources to the customers deemed to pose higher risks.
SPs can decide to outsource some of their AML/CFT obligations, however, the implications of this need to be understood, and the risks from outsourcing factored in when assessing the business-wide risks.

Ongoing Monitoring and Transaction Scrutiny[3]

Scenarios or rules built into a system could lead to triggering significant alerts, which will not necessarily lead to any actual risk being noted or an actual check needed to be carried out. Therefore, SPs are encouraged not to 'plug and play' rules and scenarios but first test for their effectiveness before rolling out and then periodically during the implementation.

This can be done through back-testing of detection rules, whereby existing rules are tested against historical data, and alerts with a significant recurrence of false positives can be phased out. SPs can also use statistical data to maximise TM rule efficiency by conducting above-the-line or below-the-line testing. This way, SPs can increase or decrease rules' thresholds to achieve the best possible threshold and parameters.

The effectiveness of a transaction monitoring tool is not gauged by the number of rules or scenarios it has, but by the conversion rate from alert to internal reporting and subsequently external reporting to the FIAU. SPs should avoid systems that generate excessive non-material alerts, as these can create a backlog of cases and increase the risk that material cases remain unaddressed.

Rules, scenarios or other monitoring should ensure that the customer profile is factored in. Otherwise, the transaction monitoring cannot be assessed as comprehensive or effective.

Once an alert is triggered, it should either be closed if no risk was observed or escalated for further scrutiny. An audit trail and a documented, justified rationale for closure are required. Moreover, SPs are encouraged to perform internal quality checks to ensure the rationale is documented and justified.

One must remember that AML/CFT controls are interlinked, and an action or reaction on a control may impact other controls. For example, if monitoring reveals alerts, red flags, or important information about a customer, this should be reflected in the Customer Risk Assessment (CRA) and may require updated customer details. This shows why monitoring should be closely connected to CRA and customer profiling.

Policies and Procedures

An overarching recommendation is that the Implementing Procedures guide and explain to SPs what is expected of their level of risk understanding and the effectiveness of the controls they implement. It may be tempting to replicate entire extracts from the Implementing Procedures for several policy documents, such as the BRA, CRA and CAP. However, this approach would not add value, and SPs should adopt a risk-based approach and implement a control framework tailored to their business and commensurate with their risk exposure.

[3] Overall, it was observed that this is one of the areas where SPs are heavily investing, especially systems driven by machine learning technology and artificial intelligence. Click here to view the Guidance note titled "A Look Through the Obligation of Transaction Monitoring"

4. SPs Who Fail to Adhere to the Requirements of the Directive

It is understood that during the implementation phase, some challenges may be encountered that may lead to changes to the previously agreed-upon action plan. However, if the changes result in ineffective controls or unnecessary delays or otherwise the management body of the SP is not committed to ensuring the corrective actions required are addressed effectively and sustainably, the Committee may decide to take additional administrative measures. SPs must understand that the imposition of a Directive is legally binding. Therefore, the actions outlined in the Directive must be implemented in a manner that is efficient, effective, and sustainable. If not, there are additional actions that the Committee may take when SPs fail to implement the necessary remediation, including the following:

Specific notification to the Prudential Regulator

The Committee would decide to inform the prudential regulator that the required actions were not being implemented, thus highlighting unaddressed gaps in the SP's controls and possible governance concerns. This may lead to the Authorities seeing the need for action on the SP's ability to keep operating without any restrictions until compliance is restored or enhanced.

Specific notification to the FIAU's Supervisory Section

Where the Committee observes risks to the effective implementation of the corrective actions, it may decide to notify the FIAU's Supervision Section, for consideration when coordinating its supervisory plan.

Administrative Penalty (including periodic penalty payments)

Where the Committee observes that the SP is not meeting the requirements of the Directive, or is not dedicating sufficient time and resources, or there are unnecessary delays in implementing the corrective actions, it may also decide to impose an administrative penalty. This is either a one-time penalty for breaching the requirements of the directive or else impose a daily pecuniary penalty which would accumulate until the SP demonstrates that compliance has been restored, in line with the requirements of the Directive.

5. Key Takeaways

10 Key Takeaways SPs should remember from reading this paper:

1. Collaboration Ensures Effective Outcomes

Active cooperation between SPs and the Corrective Actions Team is essential to ensure that Directives lead to the implementation of sustainable and effective AML/CFT controls.

2. Directives Focus on Future Compliance

The purpose of a Directive is not to assess past performance but to ensure long-term, future-oriented compliance that effectively mitigates ML/FT risks. SPs should avoid a tick-box approach when fulfilling their AML/CFT obligations. Directives should be viewed as an opportunity to collaborate with the regulator and ensure that any shortcomings are effectively addressed.

3. Proactive Engagement is Encouraged

Many SPs go beyond the Directive's requirements by initiating additional meetings and implementing wider remedial measures, showing a strong commitment to compliance.

4. Effective Documentation is Critical

Clear, concise, and relevant documentation is fundamental to demonstrate compliance efforts. It allows the Corrective Actions Team to verify that proper controls are implemented and functioning as intended.

5. Unclear or Excessive Documentation is Unhelpful

Submitting vague or irrelevant documentation, or excessive volumes without context, hinders the review process and undermines transparency.

6. Realistic Timeframes Are Key to Success

SPs must set achievable deadlines for implementing corrective measures and immediately communicate any delays or risks. Unrealistic deadlines tend to lead to failure and do not reflect stronger compliance.

7. Communication and Transparency Build Trust

Open communication, especially when delays or challenges arise, demonstrates accountability and a genuine intent to improve AML/CFT frameworks.

8. A Risk-Based Approach Must Be Maintained

SPs must tailor their controls based on customer and business risks rather than applying overly rigid or one-size-fits-all measures, such as unnecessary EDD on low-risk clients or generic measures when risks are heightened.

9. Transaction Monitoring Needs to Be Proportionate and Effective

Transaction monitoring systems should be tested for effectiveness, avoiding excessive false positives. The focus should be on the quality of alerts, not quantity.

10. Controls Must Be Interlinked and Reviewed Holistically

AML/CFT measures such as transaction monitoring, customer risk assessment, and customer due diligence must work together. Changes in one area should prompt updates across the compliance framework.

6. Concluding Remarks

The FIAU aims to identify gaps in AML/CFT measures by undertaking compliance reviews. Consequently, the Directives imposed assist SPs to remediate these gaps, thereby combating potential ML/FT while promoting good business and safeguarding Malta's reputation as a place of good standing. Considering that the criminal landscape continues to shift rapidly and evolves continuously, it is even more important to strengthen the cooperation between the FIAU and the SPs. When SPs fully cooperate and take corrective actions beyond those legally required by the Directive, they not only reinforce their operations but also contribute to safeguarding the entire jurisdiction by helping to ring-fence it against ML/FT. Collaboration with the FIAU further strengthens this impact by offering valuable insights into potential gaps in legislation or guidance, enhancing the Authority's understanding of best practices and effective control measures.

The fight against ML/FT lies at the heart of the FIAU's mission. However, this effort cannot succeed in isolation. SPs play a pivotal role in this collective endeavour, serving as a critical line of defence in detecting illicit activity and helping to deprive criminals of their ill-got gains. From the perspective of SPs, this mandates robust control frameworks that are not only compliant with regulatory requirements but are designed in a risk-based manner to ensure control effectiveness. SPs subject to Directives have an opportunity to identify and tackle control issues that remain outstanding by working together with the FIAU in an open dialogue. In turn, throughout the Directive process, the FIAU can provide meaningful recommendations on how SPs can address these areas for improvement. A good compliance culture is of the essence not only from a regulatory perspective, but from an internal governance perspective, therefore, SPs that take Directives seriously contribute towards a common goal – mitigating ML/FT in our jurisdiction.

FIAU

Annex 1 - Statistical Metrics About Directives

Annexes

Annex 1.1: Directives Imposed

Between 2020 and 2024 a total of 101 Directives were imposed following a compliance review, this from a total of 139 Administrative actions imposed on 134 SPs. An overview of the different sectors on whom a Directive was imposed is being delineated in the table below.

Sector		Remediation Directives	Follow Up Directives	Total
Financial	Credit Institution	2	13	15
	Investments	9	4	13
	Financial Institution	3	6	9
	VFAs	-	1	1
	Insurance Services	1	-	1
	Total	15	24	39
Non-Financial	Gaming (inc. Land Based)	2	9	11
	TCSPs	29	5	34
	Notaries	7	2	9
	Real Estate Agents	2	1	3
	Accountants/Auditors	3	-	3
	Advocates	2	-	2
	Total	45	17	62
Grand Total		**60**	**41**	**101**

Annex 1.2: Directives Meetings Held

Between 2020 and 2024, 262 matters were discussed across 151 meetings with SPs. The table provides a breakdown of the topics discussed by Directive Type. During these meetings, SPs provide an explanation, a status update and walkthroughs on the respective controls implemented. It is customary to discuss any challenges faced during the remediation process, where Enforcement officials provide their input and assistance as necessary.

Though meetings are held on numerous topics covering broadly all the SP's AML/CFT obligations, the focus is predominantly on those obligations where new measures would be implemented. These often include the implementation of new systems. During these meetings, SPs provide an update on the progress attained and discuss challenges or difficulties encountered when implementing these systems. System walkthroughs would also be carried out.

Topics Discussed	As part of Follow-Up Directives	As part of Remediation Directives	Total number of Matters Discussed
Customer Risk Assessment (CRA)	34	26	60
Ongoing Monitoring - Scrutiny of Transactions	36	7	43
Business Risk Assessment (BRA)	23	16	39
Client File Review Feedback	13	5	18
CDD - Purpose & Intended Nature	9	5	14
Jurisdiction Risk Assessment (JRA)	7	7	14
CDD - Identification and Verification	11	2	13
Pre-Directive Initiation Meeting	9	3	12
Policies & Procedures	7	3	10
Other Updates	4	2	8
Enhanced Due Diligence (EDD)	4	2	6
Ongoing Monitoring - Updating of documents	5	1	6
PEPs	3	3	6
Training	3	1	4
Record Keeping	3	-	3
MLRO	3	-	3
Reliance	-	1	1
Reporting	-	1	1
Outsourcing	-	1	1
Adverse Media Screening	1	-	1
Employee Screening	1	-	1
Grand Total	**176**	**86**	**262**

Annex 1.3: Directives completed

67 Directives were completed between 2020 and 2024. The table below delineates the number of Directives closed during this period.

Directive Closures Per Year	
2020	5
2021	11
2022	12
2023	19
2024	20
Total	**67**

FIAU

Annex 2 - Case Studies

Annex 2.1: Credit Institution (Follow Up Directive)

Sector	Credit Institution	
Breaches Determined	1) Business Risk Assessment (BRA)	4) Politically Exposed Persons (PEPs)
	2) Customer Risk Assessment (CRA)	5) Transaction Monitoring (TM)
	3) Purpose and Intended Nature of the Business Relationship (P&IN)	6) Suspicious Transaction Reporting (STR)
Types of Directive	Follow-Up Directive	
Number of Meetings Held	7 Directive Meetings	

Measure and Controls

	Pre-Directive	**Post-Directive**
BRA	**Inadequate BRA Methodology** • Only focused on ML risks emanating from product and jurisdiction risk, excluding other relevant ML/FT risks. • Terrorism Financing (TF) risk not considered. • Lacking assessment of the controls in place, leading to inadequate control effectiveness ratings within its BRA.	**Improved BRA Methodology** • BRA updated to cater for all relevant ML/FT risks and enhanced the quantitative analysis undertaken by making use of historical data to assess the likelihood of a risk materialising. • Included an assessment of ML/TF risks emanating from the NRA & SNRA which are directly applicable to the Bank. • Undertook an assessment of its controls and segregated the controls being applied under 19 different control categories, leading to enhanced control effectiveness rating within its BRA.
CRA	**CRAs not completed on all customers** • Operated for a period without conducting CRAs on some types of customers. **Inadequate CRA Methodologies** • Blanket approach to assigning CRA ratings to customers making use of a specific product. • Inadequate CRA ratings since risk weightings were not adequately calibrated.	**CRAs completed for all customers** • Updated its CRA methodology and updated all its customers' CRAs using the revised methodology. **Improved CRA Methodology** • Invested in an automated CRA system to compile CRAs. • Revised jurisdiction risk assessment which feeds directly into the tool. • Added additional questions and drop-downs to cover additional ML/TF risk components. Furthermore, additional questions are required to be completed depending on the type of products/ services offered. • Calibrated risk weightings and testing undertaken prior to finalising revised methodology.

P&IN	**Lacking information on customers SoW/SoF** • Depending on the product offered, different failures were noted ranging from not obtaining information and/or documentation on the SoW, nor customers occupation or detail on the origin of the initial funds.	**Enhanced SoW/SoF information and Documentation** • Revised registration forms and started requesting that all customers provide SoW/SoF information at onboarding. These details are required prior to proceeding with the application. • For legacy customers, the Bank obtained this information during ongoing monitoring reviews.
PEP Checks	**PEP screening tool did not screen all customers** • For certain products offered to its customers, PEP screening was not being conducted.	**Enhanced PEP identification measures** • Included a PEP declaration field which is embedded in the registration form for all products offered. • Automated PEP screening is also being carried out. • Legacy customers screened and required action taken on potential hits identified.
TM	**Inadequate Transaction monitoring** • Failed to monitor whether transactions were in line with the customer's business profile. • TM rules were not sufficiently calibrated to flag unexplained deviations, unusual and suspicious transactions.	**Enhanced Transaction monitoring** • Adopted a new tool designed to identify potentially suspicious or fraudulent transactions, and to highlight deviations from the customer's profile both pre- and post-transaction monitoring. • Implemented new alerts featuring terrorism financing scenarios, incorporating various thresholds segmented by product and service type, and calibrated according to the customer's risk profile.
Reporting	**Failure to report** • STRs/SARs were not submitted in cases where there were sufficient grounds to suspect potential ML/FT.	**Enhanced Reporting Procedures** • Internal and external reporting procedures were updated, including the introduction of forms to enable employees to promptly identify and escalate suspicious behaviour or transactions. • Delivered multiple internal training sessions covering topics such as money laundering, terrorist financing, and fraud.

Annex 2.2: Remote Gaming Operator (Follow Up Directive)

Sector	Remote Gaming Operator	
Breaches Determined	1) Business Risk Assessment (BRA)	4) Employee training
	2) Customer Risk Assessment (CRA)	5) MLRO
	3) Policies & Procedures	
Types of Directive	Follow-Up Directive	
Number of Meetings Held	3 Directive Meetings	
Measure and Controls		
	Pre-Directive	**Post-Directive**
BRA	**Inadequate BRA** • Lacked quantitative data pertaining to the applicable control measures and their effectiveness. • Jurisdictional risk assessments (JRA) did not provide for a final scoring, nor were the potential ML/FT risks emanating from such jurisdictions adequately assessed	**Improved BRA** • Updated to include quantitative data illustrating how controls are being effectively implemented. • JRA revised to consider, as part of the assessment, multiple relevant sources to derive the ML/FT risks posed by a particular country. A risk score per country was also completed.
CRA	**Inadequate CRA Methodology** • Did not assess customers' risk emanating from all four ML/FT risk pillars. • Was inadequately based on limited customer information being collected.	**Improved CRA Methodology** • Now incorporates an assessment covering all four ML/FT risk pillars emanating from its customers. • An initial assessment is undertaken at onboarding based on preliminary information, followed by a comprehensive assessment post-registration which incorporates additional data including actual transaction volume and patterns.

Policies and Procedures	**Inadequate Policies and Procedures** • Failed to clearly explain the information and documentation required to establish the purpose and intended nature of the business relationship and that required to compile a comprehensive profile. • Failed to explain PEP checks required and how to record them. • Failed to explain how to perform Enhanced Due Diligence (EDD) • Failed to explain how to carry out proper transaction monitoring.	**Improved Policies & Procedures** • Policies & Procedures were amended in line with FIAUs recommendations and updated copies provided.
Training	**Lack of AML/CFT Knowledge demonstrated by employees** • AML/CFT training was not adequately provided and an overall lack of knowledge on AML/CFT matters was observed.	**Improvement of AML/CFT knowledge demonstrated by employees** • AML/CFT training was delivered and corroborated by training certificates and presentation materials. • Ongoing training plan designed to ensure employees remain updated with potential emerging threats of ML/FT.
MLRO	**Inadequacy of the MLRO** • The appointed MLRO demonstrated insufficient knowledge of AML/CFT requirements. • The individual held a position with an evident conflict of interest and lacked appropriate authority and independence.	**New MLRO appointed** • Appointed a new MLRO, possessing adequate AML/CFT expertise, free from any conflicts of interest and provided with the required authority and independence.

Annex 2.3: TCSP (Remediation Directive)

Sector	Trustees & Fiduciaries - Company	
Breaches Determined	1) Business Risk Assessment (BRA)	2) Customer Risk Assessment (CRA)
Types of Directive	Remediation Directive	
Number of Meetings Held	2 Directive Meetings	
Measure and Controls		
	Pre-Directive	**Post-Directive**
BRA	**Failures surrounding the BRA** • Did not include quantitative data as part of the assessment to identify potential ML/TF risks to which the business may be exposed. • The effectiveness of the mitigating measures was not assessed. • Jurisdiction risk assessment was not conducted.	**Improved BRA** • Which incorporates quantitative data as a risk driver in determining the likelihood of risk materialisation. • Includes a detailed analysis of the control effectiveness, with a clear rationale for each control rating. • JRAs are now being conducted using specialised compliance software, based on reliable sources and considering various types of potential ML/TF risks a particular jurisdiction may pose.

CRA	**Failures surrounding the CRA**
	• The CRA methodology was inadequate, with identified shortcomings in assessing the ML/TF risk emanating from customer, geographical, and product risk.
	• Instances were identified where no CRAs were conducted for customer files.
		CRA Enhancements
		• CRAs are now automated
		• Methodology incorporates multiple risk parameters and sub-parameters covering all relevant potential ML/FT risk exposure emanating from its customers, including:
		  ◦ Geographical risk enhanced to cover material links the customer may have to specific jurisdiction(s)
		  ◦ Product risk now considers the inherent risk of the products/services.
		  ◦ Customer risk evaluates a wider range of factors, including industry, source of funds, and adverse media.
		• A formal declaration was provided to confirm that CRA assessments were completed for all customers.

Annex 2.4: Notary (Remediation Directive)

Sector	Notary	
Breaches Determined	1) Customer Risk Assessment (CRA)	3) Identification & Verification
	2) Policies & Procedures	4) Politically Exposed Person (PEP) checks
Types of Directive	Remediation Directive	
Number of Meetings Held	1 Directive Meeting	
Measure and Controls		
	Pre-Directive	**Post-Directive**
CRA	**Failure to conduct CRAs** • Did not have CRA methodology • CRAs were not conducted for a number of customer files reviewed.	**Enhancements to CRA** • CRA methodology established with the help of a third-party provider. • CRAs completed for each client using the newly established methodology. • Notary can now operate risk-based and request additional documentation commensurate with the customer's assigned risk level.
Policies & Procedures	**Policies & Procedures found to be insufficient** • Lacked formal risk management procedures. • Lacked procedures relating to EDD measures	**Improved Policies & Procedures** • Policies & Procedures were amended according to the FIAU's recommendations, and updated copies were provided.
ID&V	**Lack of Verification of Customers' information** • Instances were identified where customers' details were not verified.	**Verification processes improved** • Missing verification documents were collected for the identified cases. • Policies & Procedures updated to document the required verification process.
PEP checks	**Failure in Identifying and Mitigating Risk on PEPs** • Lack of measures in place to determine whether customers are politically exposed.	**Improved Identification Measures on PEPs** • Invested in an external third-party system, used to screen customers. • Legacy customers screening undertaken and appropriate action taken where necessary.

Annex 2.5: CSP (Follow-Up Directive) (Case-specific Scenario)

Sector	CSP
Breaches Determined	Transaction Monitoring (TM)
Types of Directive	Follow-up Directive
Number of Meetings Held	1 Pre-Directive Meeting | 4 Directive Meetings
Case specific scenario	The FIAU requested an in-person meeting with the CSP, requesting that they come prepared to explain a complex activity identified during the customer file review.
Case Description	Phase 1 of the Directive involved a walkthrough of the systems in place, with a review of the CSPs' policies and procedures governing transaction monitoring (TM). In Phase 2, to evaluate the effectiveness of these controls, a sample of client files was requested for detailed review. Multiple unstructured documents related to the selected customer files and their transactions were submitted. Enforcement officers reviewed the extensive material and sought clarification from the CSP to confirm that proper scrutiny had been applied. This was necessary because, on initial review, it appeared that potentially suspicious activity and complex legal arrangements may not have been adequately examined. Despite several attempts to understand the customer's activity and the CSP's analysis, the responses received were incomplete and did not provide sufficient clarity. At this stage, the enforcement section and the CMC were dissatisfied with the explanations and evidence provided by the CSP, as it had failed to provide reassurance that the required remediation had taken place. This led to requesting an in-person meeting with the CSP to provide a platform for the CSP to communicate and provide detailed explanations of the scrutiny undertaken on a particular customer. This was required to clarify whether the CSP had implemented the required controls, to understand what the CSP did to analyse the complexity and why nothing suspicious was noted. During the two-hour meeting, the CSP's representatives provided more detailed explanations, explained the relevance of specific documentation and ascertained that the required controls had been applied. Following this meeting, the SP provided additional detailed written explanations and further supporting documentation, which allowed the enforcement officials to close any remaining gaps and conclude their file review.

Key Takeaways	SPs should submit well-structured documentation and clearly explain the documents provided and the reasons for each. This approach facilitates the smooth processing of the Directive and helps minimise unnecessary back-and-forth. When documentation pertains to complex structures, transactions or arrangements, SPs should ensure adequate documentation of the analysis conducted to ensure that clients are not facilitating illicit activity.

Questions on this document or on the application of AML/CFT measures may be sent to queries@fiaumalta.org

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq l-Mdina,
Central Business District Birkirkara, CBD 2010

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org