FIAU

The Business Risk Assessment

Issued: 9th April 2021

CONTENTS

1. INTRODUCTION

The carrying out of a business risk assessment (BRA) is an obligation that came into force as from 1st January 2018 and stems from Regulation 5(1) of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) and Section 3.3 of the FIAU Implementing Procedures Part I (IPs). However, the exercise of conducting a thorough BRA has benefits that go beyond mere compliance with regulations.

In essence, the BRA is the foundation of the risk-based approach, which requires the varying and adapting the application of anti-money laundering and combating the funding of terrorism (AML/CFT) measures, policies, controls, and procedures. This is necessary to ensure that resources are applied in areas where there is a higher-than-normal risk of ML/FT. For instance, if a subject person offers several types of products, with one product being more susceptible to ML/FT, then it stands to reason that enhanced controls should be applied in the provision of this product. In turn, those controls should also be better suited to address and mitigate the particular risk identified. However, this cannot be effectively applied unless the subject person identifies and assesses its exposure to ML/FT risks and understands what the various risks are and how they may manifest themselves.

Therefore, the starting point to guiding resource allocation, as well as the level, timing, and type of controls, lies entirely on conducting an effective BRA.

2. ANALYSIS OF THE BRAs CARRIED OUT ACROSS MALTESE INDUSTRIES SUBJECT TO AML SUPERVISION

In 2020, the FIAU carried out a review of BRAs drawn up by subject persons operating within the different sectors and sub-sectors, through which an analysis of key elements was undertaken. The objective of this document is to publish insights into common trends and shortcomings in relation to the obligation to carry out a BRA. This will assist subject persons to identify areas within the BRA that can be improved for the purpose of better understanding and mitigating their ML/FT exposure. The results of the analysis exercise are based on:

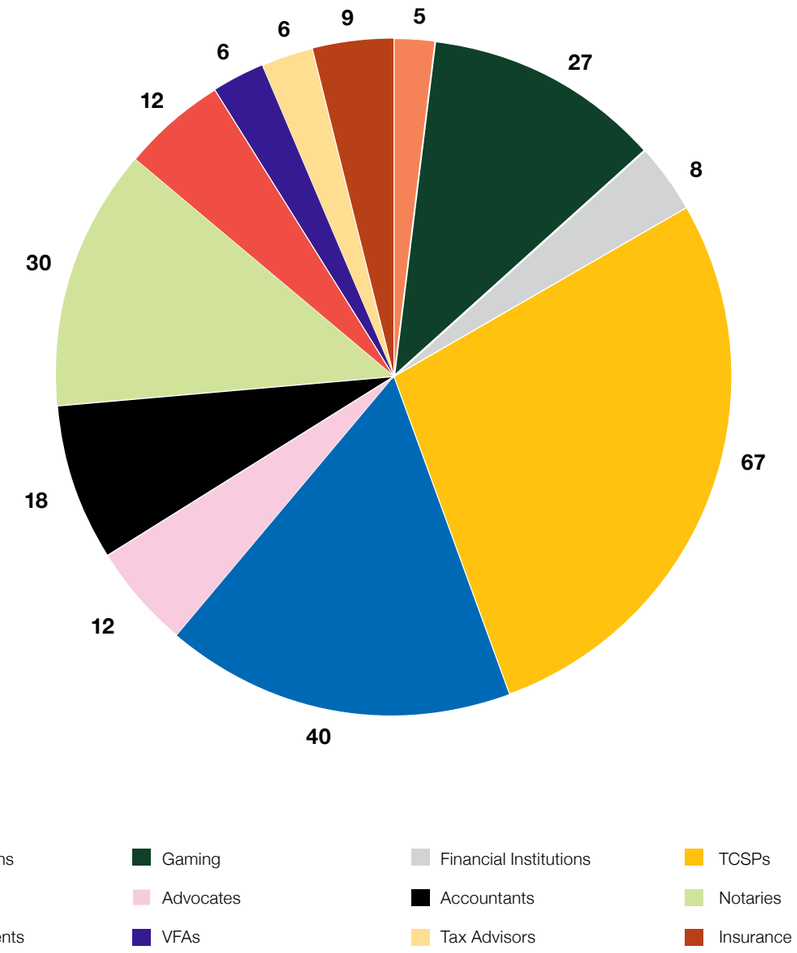
a. A high-level review of 240 BRAs, representing a sample of the BRAs submitted by subject persons as part of the 2020 Risk Evaluation Questionnaire (REQ) submission exercise[1] (the High-Level review).

b. An in-depth analysis of 100 BRAs, representing a sample of the BRAs provided by subject persons as part of AML/CFT compliance examinations carried out by the FIAU, MFSA and/or MGA[2] during the period 1 July 2019 to 30 June 2020 (the in-depth review).

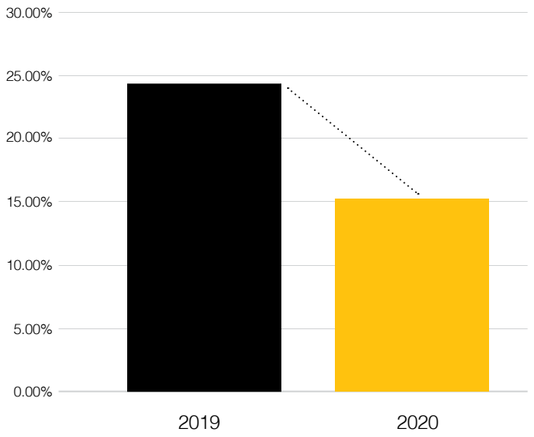
1. Subject persons are required to submit a copy of the BRA on an annual basis as part of the annual REQ submission. The deadline for the submission of the 2020 REQ was 18 May 2020.
2. The MFSA and MGA carry out AML/CFT examinations as appointed agents of the FIAU on its behalf in terms of Article 27(3) of the Prevention of Money Laundering Act.

3. RESULTS OF THE HIGH-LEVEL BRA REVIEW

The following charts show the distribution of the sample across the different sectors, and the percentage of the sector population that the sample represents. The objective of the high-level review was to assess the BRA content in terms of risk and controls, and to assess the methodology used by subject persons in carrying out the BRA.



BRA non-submission



On a positive note, following the 2020 REQ submission exercise, the FIAU noted a decrease of 9.1% in the number of subject persons that did not carry out a BRA when compared to the 2019 REQ submission exercise. In fact, whereas, in 2019, 24.3% of subject person population did not carry out a BRA, from the 2020 REQ submission exercise it was concluded that this decreased to 15.2%. Table 1 outlines the percentage of subject persons per sub-sector that did not submit a BRA, and the overall submission rate, comparing 2019 to 2020 (as at May 2020). The FIAU noted that all sub-sectors experienced an increase ranging between 10% to 27% in the total number of subject persons who carried out a BRA as part of the 2019 REQ submission exercise, with real estate agents increasing the BRA submission rate by 27%.

> **Without a clear methodology, subject persons run the risk of attaining inaccurate results and in turn an inappropriate assessment of risks and controls.**

Key Statistics

27%
Increase in submissions in the **real estate** sector

100%
Submission rate by **Credit Institutions** in 2020

89%
Submission by **VFAs** in their **first year** as subject persons

Table 1

Sectors	2019 REQ		2020 REQ	
	BRA in place?			
	Yes	No	Yes	No
Credit Institutions	96%	4%	100%	0%
Financial Institutions	80%	20%	94%	6%
Trust and Company Service Providers (TCSPs)	80%	20%	90%	10%
Gaming	71%	21%	87%	13%
Investments	83%	17%	93%	7%
Accountants/Auditors	65%	35%	80%	20%
Advocates	44%	56%	57%	43%
Notaries	77%	23%	89%	11%
Real Estate Agents	46%	54%	73%	27%
Virtual Financial Assets Agent (VFAs)*	N/A	N/A	89%	11%

3.1 BRA METHODOLOGY

Requirement: Section 3.3.2 of the IPs requires the BRA to include a description of the methodology adopted by subject persons in carrying out the BRA. Section 3.3.1 of the IPs also explains that the BRA should define the residual risk by considering the inherent risk level across the array of ML/FT risks in the light of the effectiveness of controls applied to mitigate these risks.

The analysis of the sampled BRAs concluded that a good number of BRAs met the FIAU's expectations by adopting a detailed methodology that clearly explains the approach used to determine the inherent risks and control effectiveness. However, some subject persons did not include a methodology specifying the approach used in carrying out the BRA. Similarly, instances were noted where the BRA did not explain how the likelihood and impact level for each inherent risk and the control effectiveness level were calculated. Furthermore, some of the sampled BRAs did not include a description of how controls correlate with the respective risks, that is, how the control measures serve to mitigate the specific risks identified.

*VFAs were not yet subject persons during the REQ 2019 reporting period

The FIAU expects the BRA to include a description of the method used by subject persons to conduct the risk assessment. Furthermore, a clear and adequate methodology which sets out how to assess the likelihood and impact of the identified risks, and how to assess the effectiveness of the respective controls needs to be included. Without a clear methodology, subject persons run the risk of attaining inaccurate results and in turn an inappropriate assessment of risks and controls. This may lead subject persons to erroneously disregard areas which present high ML/FT risks. Equally concerning, this could also lead to focusing on areas incorrectly determined to pose high ML/FT risks, leading to inefficient use of resources.

3.2 ML/FT RISKS AND CONTROLS

Requirement: Regulation 5(1) of the PMLFTR and Section 3.3.1 of the IPs require subject persons to identify and consider risk factors relating to customer risk, geographical risk, products, services and transaction risk and delivery channel risk. The IPs further state that risk factors should be considered from both a qualitative and quantitative perspective and provide guidance on how this can be done.

Through an analysis of the different risk categories included within each of the BRAs reviewed, the FIAU noted the following:

- Most subject persons have adequately identified and assessed inherent risks in relation to the risk categories mentioned in Regulation 5(1) of the PMLFTR, namely, those associated with the customer types, the jurisdictions to which customers are connected, the products and services offered as well as the channels used to distribute the latter.

- Some BRAs were expected to include further detailed explanation of the specific risks and how these can manifest themselves, since the inherent risks listed were too broad in nature.

- When it comes to analysing risks from a quantitative perspective, some BRAs did not include such an assessment and focused only on the qualitative perspective. It is important that subject persons do not rely solely on a list of inherent risks but should also determine how numerous these risks are within their operations, as this has a bearing on the risk exposure.

- The definition of inherent risks and residual risk and how these are to be calculated was at times misunderstood by subject persons. The inherent risk is the level of ML/FT risk before the application of controls to mitigate the risk and is calculated by determining the likelihood and impact of the risk. On the other hand, the residual risk is the level of ML/FT risk after applying the controls to reduce the risk.

When it comes to the controls put in place by subject persons to mitigate the existing risk factors, most of the sampled BRAs did mention the controls currently in place. However, the FIAU noted that some of the BRAs do need to be enhanced, by including an explanation on how the controls are applied, and how these controls serve to lower the inherent risk.

4. BRA GOOD PRACTISES

During supervisory examinations, the subject person's BRA document is evaluated based on the analysis of ML/FT risks and the respective controls vis-à-vis the subject person's business model, operations, client base and application of AML/CFT control measures. These assessments often reveal a number of deficiencies in the BRA documents.

The section hereunder sets out some best practises to ensure that Business Risk Assessments meet the FIAU's expectations:

The BRA should be specific to the subject person

The BRA document should not be an off-the-shelf document, but rather a tailored made document that reflects the subject person's own business model, operations, and scenarios. The FIAU positively noted that there has been an increase in the number of subject persons that engaged consultants to assist in carrying out the BRA. Subject persons are reminded to actively participate and own the work carried out by others, to ensure that the risk assessment reflects their own circumstances, activities and specificities. Likewise, should a subject person adopt the BRA of another entity operating within the same group structure, it is imperative that the BRA is updated to reflect the subject person's own circumstances, especially as different entities within the group may offer different products or services and to different customer categories.

Subject persons should understand their own BRA

In instances where the preparation of the BRA is outsourced to third parties, supervisory examinations occasionally concluded that subject persons had minimal understanding of the BRA and, particularly of the inherent risks to which the business is exposed to. The FIAU acknowledges the subject persons' commitment to engage consultants to assist them in carrying out certain AML/CFT obligations. However, subject persons remain solely responsible for the BRA and most importantly should ensure that they have knowledge of both the content and result of it. The BRA should not be interpreted solely as an exercise that has to be conducted to be in line with the obligations stipulated in the PMLFTR and IPs. Rather, it should be perceived as a tool that allows subject persons to be aware of their risk exposure, to determine how risks can be mitigated to an acceptable level, and to determine the areas to prioritise in terms of AML/CFT.

> **Subject persons remain solely responsible for the BRA and most importantly should ensure that they have knowledge of both the content and result of it.**

Subject Persons should understand the BRA methodology

From discussions held during supervisory examinations between the subject person's officials and the FIAU, the MFSA and MGA (as agents of the FIAU), the FIAU concludes that most subject persons have a good understanding of the process used to carry out the BRA, while others require some improvement. It is imperative that subject persons challenge and understand the methodology used to carry out the BRA, to ensure that this is effective in deriving correct results. The FIAU is providing insights and examples of poor practises noted:

- The IPs provide detailed explanations and different methodologies that can be adopted to conduct the BRA. However, it is up to the individual subject person to determine which approach to apply in carrying out the BRA, as long as the methodology is effective in obtaining correct and accurate results. In one case, the scores given for the inherent risk likelihood and inherent risk impact were determined to be low for every risk factor. Based on the FIAU's assessment, it was considered highly unlikely that each risk factor would have a low likelihood of occurring and a low impact if the situation occurs. In fact, the FIAU concluded that the inherent risk result was far lower than it should have been. In turn this affected the other elements of the risk rating, namely the mitigating measures, the residual risk, and whether the residual risk falls within the subject person's risk appetite. In another case, the BRA methodology consisted solely of taking the average risk of the client base risk rating, rather than initiating the BRA through the identification and assessment of the risk factors posed by the business.
- Similarly, the rationale behind the low, medium, or high-risk rating is at times not explained, and no indication is given as to what factors were considered for the purpose of deriving the risk rating (e.g., likelihood or impact of the inherent risk). This applies especially when the risk rating of specific inherent risk factors differs significantly from the standard level of risk typically associated with that factor. For instance, the use of cash is associated with a higher level of ML/FT risk. If the use of cash is listed as posing a low inherent risk, the subject person is expected to justify this by documenting the elements that were taken into consideration.

All evident risks should be included

Subject persons should strive to include all apparent and important risks, as overlooking any risks could lead to incorrect results. For example:

- In the case of a subject person that mainly targets customers owning significant immovable property assets, investment portfolios, yachts and aviation jets, the BRA should assess the risks relating to High-Net-Worth Individuals (HNWI).
- If the majority of a subject person's operations involves the provision of directorship services, this should be adequately considered in the BRA.
- Subject persons actively involved in operations involving high cash flows should not overlook the risks arising from the use of cash.
- Subject persons that opt to outsource some of their customer due diligence (CDD) obligations to third parties, should assess and include this risk exposure in their BRA.

Therefore, prior to concluding the BRA, subject persons should confirm that all relevant risks have been adequately incorporated in their assessment. This can be achieved by inviting key personnel from various departments to participate in the identification of ML/FT risks and by ensuring that the MLRO participates in the drafting of the BRA.

Avoid generic mitigating measures

The AML/CFT controls listed in the BRA should be well defined and should clearly explain how they serve to mitigate the associated risks. For instance, one BRA listed the mere application of CDD measures as a safeguard against the risks arising from exposure to Politically Exposed Persons (PEP). However, this is not sufficient given that CDD measures are to be applied in all circumstances irrespective of the risk level. In cases such as the above, subject persons are expected to define in more detail the type of Enhanced Due Diligence measures to be applied (e.g. an explanation of what source of wealth information would be requested and an explanation of the enhanced ongoing monitoring mechanisms to be applied). It is likewise important that the correlation between the controls and the specific risks mentioned in the BRA is clear and well-defined.

BRA should reflect the actual control measures adopted

When the BRA refers to a set of controls that subject persons are to apply to mitigate the identified risks, the FIAU expects subject persons to eventually apply these controls. During the course of compliance examinations, the FIAU, or the MFSA and MGA (as agents of the FIAU) identified instances wherein the controls defined in the BRA were not applied. In some cases, subject persons explained that the introduction of such controls was in the pipeline or a work in progress. Whilst reference to a control measure which is yet to be introduced and implemented may be made in the BRA, such controls shall not be taken into consideration for the purpose of determining the residual risk ratings. It is imperative that the BRA depicts a true picture of the subject persons' activities, the perceived risks and the controls applied at the time when the risk assessment is carried out.

The level of control effectiveness should be adequately concluded

The FIAU welcomes the fact that most subject persons have strong control measures in place to mitigate their respective risks. Having said that, the type and level of controls applied should always justify any high effectiveness rating assigned in the BRA. For example, if internal audit reports conclude that the control mechanisms implemented do not satisfactorily address the respective risks, the BRA should be mindful of this, and should not state otherwise, since this will in turn result in an incorrect low residual risk rating.

Reference should be made to the National and Supra National Risk Assessment (NRA and SNRA)

The FIAU expects BRAs drawn up by subject persons to refer to the risks and results concluded by the NRA and SNRA. It is not sufficient to merely refer to the NRA and SNRA in the introductory part of the BRA document. The BRA should provide a clear explanation of how the assessments were used as sources of information when identifying and assessing risk factors. Furthermore, when certain risks assessed by subject persons are not in line with the outcome of the NRA or SNRA, the rationale for the divergences should be documented. For example, if the latest NRA concludes that the provision of a particular service exposes the subject person to a higher ML/FT risk, the FIAU expects this to be reflected in the BRA. If the BRA, in turn, states that the inherent ML/FT risks stemming from the provision of this same service is low, the FIAU expects the subject person to explain the factors that led to this conclusion. The NRA and SNRA are important sources of information that should be consulted when conducting the BRA. Consequently subject persons should be cautious about ignoring or overruling the conclusions without reasonable justifications.

The calculation of residual risks is essential

BRAs should include a calculation of the residual risk posed by the individual inherent risk factors, as well as the overall residual ML/FT risk to which the business is exposed. The FIAU has come across cases where the overall residual risk is not calculated, while in other cases, the residual risks of individual risk factors were missing. Another shortcoming noted in some of the BRAs reviewed included a negative residual risk rating, implying that there is no ML/FT risk at all, which is practically impossible, as not all risks can be eliminated completely. The FIAU expects the BRA to include a clear indication as to whether the residual risks for each risk factor fall within the subject person's risk appetite, and whether the subject person intends to apply further mitigating measures to bring the residual risk within acceptable levels.

The BRA should be revised and updated

It is a known fact that risks are dynamic and the business model and external environment in which subject persons operate is fluid. For these reasons, the BRA should be reviewed regularly and kept up to date. Unless this is fully understood by subject persons, there is a probable risk of the BRA not reflecting the actual scenarios in which subject persons are operating. This will lead to outdated results that do not reflect the risks to which the subject person is exposed. It is positive to note that most subject persons provided the supervisors with a copy of their BRA and demonstrated that it is treated as a live document which is updated as risk scenarios change. On the other hand, there were some rare cases where the BRA fell short of reflecting the subject person's current scenarios. For instance, following the first version of the BRA, a subject person launched new products or services, but these new activities were not incorporated in the BRA. The new products and services significantly changed the risk profile of the subject person and certainly needed to be included in the assessment, together with an assessment of the controls that would serve to mitigate these new risks. Similarly, an internal audit assignment conducted by a subject person following the first version of the BRA highlighted several inherent risks which were not considered. Nonetheless, the subject person did not revise the BRA accordingly. Subject persons are reminded that even if business operations have not undergone major changes, it is important that they set out an annual review process to determine whether their current BRA is valid and current.

> **"The BRA should be reviewed regularly and kept up to date. Unless this is fully understood by subject persons, there is a probable risk of the BRA not reflecting the actual scenarios in which subject persons are operating.**

The BRA should be driven by data

Subject persons should avoid approaching the BRA exercise purely from a theoretical viewpoint by considering only threats and vulnerabilities from a qualitative perspective. It is expected that the BRA also considers risks from a quantitative viewpoint as this has an impact on the level of risk. This should be performed by considering the risk factors stemming from the current client portfolio. For instance, whereas servicing HNWIs and PEPs presents a high level of risk, subject persons are required to assess and quantify this risk by analysing just how many HNWIs and PEPs form part of their own client base. Similarly, it is not sufficient to determine which countries are non-reputable, high risk, medium risk, or low risk; subject persons should evaluate this in terms of their own client portfolio.

The BRA should be ML/FT focused

Subject persons are reminded that the BRA carried out in terms of the PMLFTR and the IPs should be ML/FT focused. Whilst subject persons may find it beneficial to carry out other risk assessments also to consider risks arising from a business, operational and financial perspective (e.g. security risks), this should not be done to the exclusion of the ML/FT perspective.

The BRA conclusions should be applied into practice

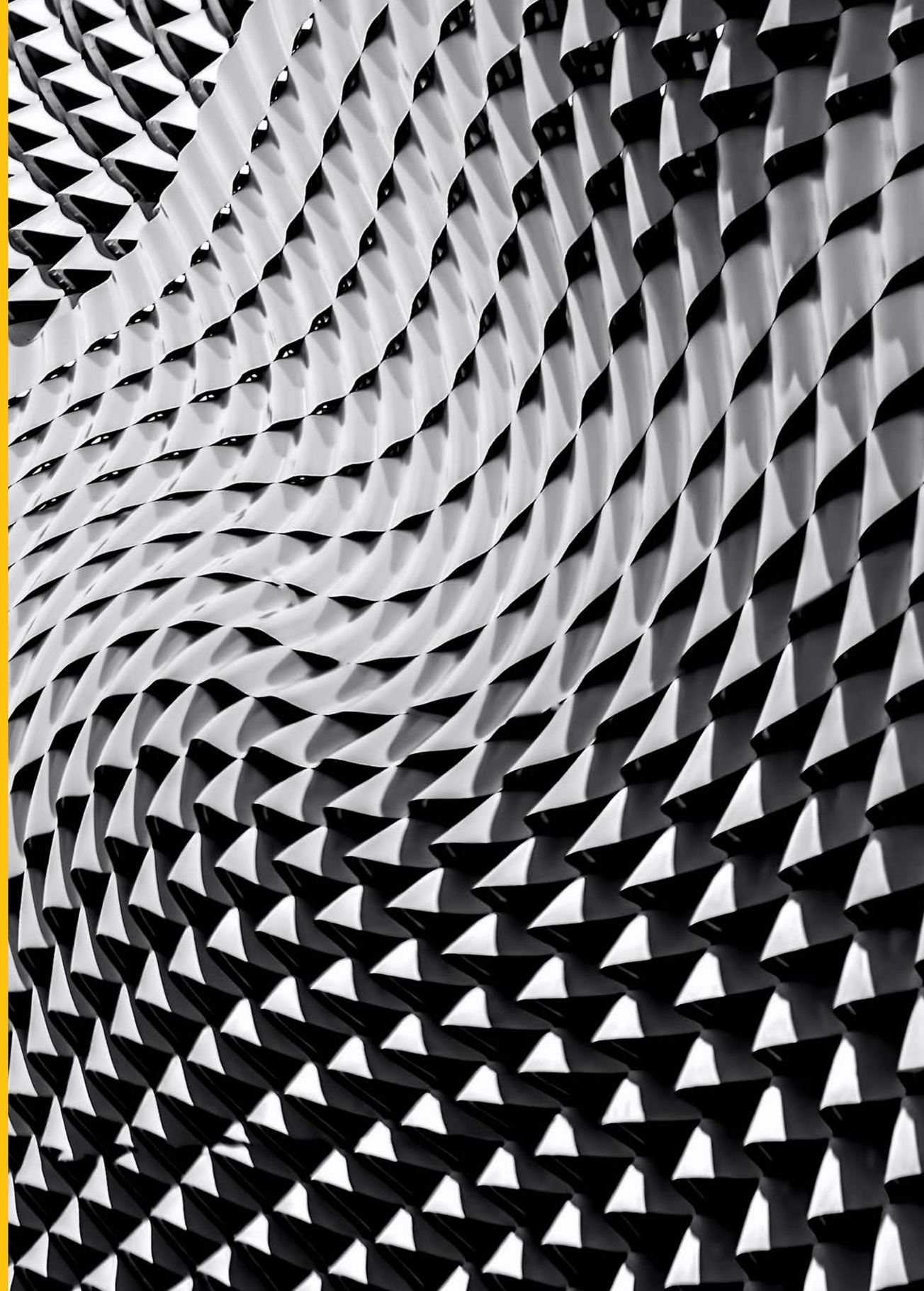
It is of utmost importance that conclusions reached in the BRA are applied throughout the subject person's AML/CFT framework. Consequently, mismatches between the results of the BRA and the application of such results must be avoided. For instance, if the BRA defines the risk of products or jurisdictions as being high, then the customer risk assessment methodology should treat those products or jurisdictions in the same manner. Similarly, the subject person's policies and procedures as well as the application of specific controls should be consistent with the description of the controls as described in the BRA. Unless the BRA results are applied consistently throughout the AML/CFT framework, the purpose behind conducting the BRA is lost.

5. CONCLUSION

The BRA is defined as being the foundation of the risk-based approach. Like any other foundation, unless the BRA is effectively carried out, there is a serious and real risk that all the other AML/CFT control structures will be misaligned or weak. Subject persons should not see the BRA solely as an obligation imposed by law. Rather, the BRA should be looked upon as an informative tool that allows subject persons to understand the main ML/FT risks present within business operations. It is also a guiding tool that assists subject persons in establishing what mitigating measures should be applied to maintain residual risks at an acceptable level. The FIAU Implementing Procedures Part I provide detailed guidance on the carrying out and review of the BRA, including information on risk factors and guidance on different methodologies.

Whilst it is acknowledged that most subject persons invested in drafting and implementing an effective BRA, the reviews carried out by the FIAU, and the MFSA and MGA (as agents of the FIAU) concluded that there is room for further improvement. To this end, the FIAU encourages all subject persons to review their BRAs and assess whether any of the above-mentioned shortcomings are present and if so, determine what steps can be taken to address these shortcomings and in turn create a more effective BRA.

FIAU | MFSA MALTA FINANCIAL SERVICES AUTHORITY | mga MALTA GAMING AUTHORITY



65C, Tower Street,
Birkirkara BKR 4012,
Malta

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

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

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