



**THEMATIC REVIEW:
BUSINESS RISK ASSESSMENTS
Report of Findings**

Table of Contents

Executive Summary.....	1
Glossary of Terms.....	3
Rationale.....	5
Purpose.....	5
Methodology.....	5
Sample.....	6
Regulatory Requirements.....	6
Findings.....	7
Section A: Understanding Inherent Risk, Mitigating Measures & Controls, and Residual Risk.....	7
Section B: Business Risk Assessment Methodology.....	10
Section C: Comprehensive Assessment of Relevant Risk Categories.....	12
Client Risk.....	13
Geographical Risk.....	14
Legal Services and Transactions Risk.....	15
Delivery Channels Risk.....	16
Section D: Adequate Quantitative Data.....	17
Section E: Governance.....	18
Conclusion.....	19
Next Steps.....	21

Executive Summary

During the first half of 2022, CARA conducted a thematic review of business risk assessments (“BRAs”) implemented by firms within its supervised population. This review assessed a total of 41 BRAs representing seventy-seven percent (77%) of supervised firms.

A well-constructed AML compliance framework begins with a robust BRA. A robust BRA is one which thoroughly examines, identifies, and assesses a firm’s inherent risk of becoming involved in, or otherwise facilitating, money laundering, terrorism financing, and proliferation financing. The results of this core exercise in determining the level of inherent risk, should then feed into and inform a firm’s policies, procedures, and controls, whilst also taking into account the firm’s risk appetite and tolerance.

Without a comprehensive and robust BRA process, a firm may fall short in implementing appropriate policies, procedures and controls that will effectively manage or, where necessary, mitigate its ML/TF/PF risks. Additionally, a firm will not be able to sufficiently evidence to CARA that it understands how, and to what extent, it is vulnerable to ML, TF, and PF. BRAs facilitate a risk-based approach, enabling firms to understand and acknowledge their ML/TF/PF risks, identify the areas that generate higher risk and on which they can then focus resources.

This report summarises the main findings from the thematic review and illustrates both good and poor practices in carrying out a BRA. It also sets out and clarifies CARA’s expectations for compliant and effective BRAs.

At the outset of the review, the majority of supervised firms were able to provide CARA with a copy of their BRA. The BRAs revealed that firms have established mechanisms to assess their ML/TF/PF risks. It was also evident there was a good understanding by firms of the purpose and objectives of the BRA. It was pleasing to find most firms addressed the key risk categories of clients, legal services, transactions, geography, and delivery channels.

Given that firms are required to conduct a BRA appropriate to the nature and size of their practice, it was expected that CARA would find BRAs varying in length, format, and structure. Smaller firms engaged in RFB matters on an occasional and or infrequent basis documented shorter and more concise BRAs. Whereas BRAs of larger international firms, with a higher volume and wider range of RFB matters, tended to be more detailed analysing likelihood and impact, financial crime risk scenarios, and included risk matrices.

Notwithstanding the above, the overall robustness of the BRAs varied considerably across the supervised population. A lack of consistency in both method and content of BRAs made reviewing, comparing, and evaluating the BRAs to draw out meaningful findings, a considerable challenge. Whilst there is no one-size-fits-all in the approach to conducting a BRA, not all included an assessment of inherent risk which is a fundamental principle in a BRA. Additionally, not all BRAs evidenced an objective assessment based upon quantifiable data.

It was further revealed when comparing the content of BRAs with information held by CARA such as firm registration records, AML Return data, supervisory engagement material, and with the firms’ own websites, that a significant minority of BRAs did not match with the type and volume of RFB client matters previously reported to CARA and the legal services being marketed by the firm.

The outcome of this review identified several key areas in which improvements are needed:

- **Documenting and applying an appropriate BRA methodology**
Not all BRAs detailed the steps taken in carrying out the risk assessment. Several instances were noted where the methodology applied resulted in an understated overall risk exposure. Over a third of BRAs drew conclusions that were not aligned to the findings of the NRA, 2015 (in place at the time) and did not provide any justification for the variances.
- **Understanding and evaluating inherent risk**
Identifying and assessing inherent risk should be the starting point when undertaking a BRA. It was noted over a third of BRAs did not refer specifically to inherent risk.

- **Conducting a TF and PF risk assessment**

Nearly all of the BRAs reviewed failed to provide an assessment of firms' risks pertaining to TF and PF. Some BRAs addressed TFS risk but with minimal analysis.

- **Requirement to test the effectiveness of controls**

The majority of BRAs which included calculations of residual risk did not adequately describe the specific internal risk controls implemented and/or did not assess the quality of controls. Only approximately 10% of BRAs provided an actual rating of effectiveness for the controls in place.

- **Providing sufficient quantitative data to support conclusions drawn**

Firms should seek to support and substantiate assertions in the BRA as much as possible with quantifiable data. Only 5% of BRAs included sufficient quantitative analysis that was in line with the size and nature of the firm's business. Relying primarily on qualitative analysis, with limited to no quantitative analysis, may potentially impede the ability to have an in-depth understanding of the ML/TF/PF risks.

- **Determining overall inherent and residual risk**

BRAs should document a clear overall conclusion and rating of the firms' ML/TF/PF risks. This may be from an inherent risk only or both inherent and residual risk standpoint depending on the methodology applied. Approximately 10% of BRAs did not provide a conclusion of the overall level of risk.

- **Implementing good governance**

Over a third of BRAs failed to evidence senior management engagement and approval. A BRA is a living document, yet over half of BRAs failed to demonstrate that the firm had a mechanism in place to conduct regular reviews of its BRA. Very few BRAs referred to internal distribution of the document and the raising of staff awareness of the firm's inherent ML/TF/PF risks.

A BRA should not be regarded as a check the box exercise. It is a valuable tool which can help drive change and prioritisation within a firm, identify deficiencies in AML/CTF/CPF controls, and improve risk awareness across staff. It is also central to a strong financial crime compliance framework.

Whilst this report does not impose new regulatory obligations, firms should assess where there are gaps and weaknesses in their BRAs and make the necessary adjustments. CARA will consider how firms have incorporated the findings from this report as part of its ongoing supervision and monitoring.

Finally, we take this opportunity to thank all the firms which submitted their BRA for review. We appreciate your cooperation, and it is hoped all firms find this report useful when undertaking, reviewing and or updating their BRA.

Clare Guile
Head of CARA
August 2022

Glossary of Terms

AMLRs	Anti-Money Laundering Regulations (2020 Revision)
BRA	Business Risk Assessment for the purposes of the AMLRs. Also commonly referred to as a practice (or firm) wide risk assessment or entity level risk assessment.
CARA	Cayman Attorneys Regulation Authority
CARA'S GUIDANCE FOR THE LEGAL SECTOR: AML/CFT/CPF/TFS	Available to view here .
LEGAL SECTOR RISK ASSESSMENT	Available to view here .
DOMESTIC FIRMS	Law firms physically located in the Cayman Islands with no branches and or presence internationally.
FATF	Financial Action Task Force
HNWI	High Net Worth Individual (Section 2 of the Securities Investment Business Act (2020 Revision) defines "high net worth person" as an individual whose net worth is at least \$800,000 KYD or its equivalent in any other currency; or any person that has total assets of not less than \$4,000,000 KYD or its equivalent in any other currency.)
INHERENT RISK	Defined as the level of risk that exists before any controls or mitigating measures are put in place.
INTERNATIONAL FIRMS	Law firms physically located in the Cayman Islands and that also have an established office(s) and or presence outside of the Cayman Islands.
MITIGATING MEASURES	Methods used to reduce the overall inherent risk.
ML	Money Laundering
NRA	Cayman Islands National Risk Assessment (2021). Available to view here .
PEP	Politically Exposed Person
PF	Proliferation Financing
PF ASSESSMENT	Proliferation Financing Threat Assessment (May 2020)
QUALITATIVE	Data that is interpretation-based, descriptive, and relating to language.
QUANTITATIVE	Data that is numbers-based, countable or measurable.
RESIDUAL RISK	The remaining level of risk following the development and implementation of mitigating measures and controls.
RFB	Relevant Financial Business as defined in the Proceeds of Crime Act (2020 Revision), Schedule 6.

RISK APPETITE	A firm's risk capacity – the maximum residual risk a firm will accept after controls are put in place.
RISK TOLERANCE	The acceptable amount of deviation from the firm's risk appetite
SUPERVISED POPULATION	CARA's register of supervised firms conducting relevant financial business.
TF	Terrorism Financing
TF NRA	Cayman Islands Terrorist Financing National Risk Assessment (February 2020)
THEMATIC REVIEW	An in-depth analysis of our supervised population's BRAs conducted by CARA to produce valuable insights.
TRANSPARENCY INTERNATIONAL	An international non-governmental organization. TI's Corruption Perceptions Index (CPI) reveals corruption levels at an international level and is a useful tool.
ULTRA HNWI	Ultra-High Net Worth Individual - An "ultra-high net worth person" is an individual whose net worth is over \$30,000,000 USD.

Rationale

A business risk assessment (“BRA”) is the foundation of an AML¹ compliance framework and should support and drive a firm’s risk-based approach. We therefore chose BRAs as the topic of our first thematic review based on the importance of getting the BRA right.

Why is it so important? If a firm fails to objectively examine and understand its potential exposure to ML/TF/PF then it can have grave consequences. Without an adequate and proper BRA, there is a risk a firm may fail to implement appropriate policies, procedures, and controls to monitor, manage and, where necessary, mitigate its ML/TF/PF risks. Law firms play a key role as gatekeepers of the financial and legal systems, helping to protect the public from the harm caused by ML/TF/PF, and ensuring the Cayman Islands is a clean and safe place to do business. The adverse publicity of being connected in any way with financial crime is not only damaging to a firm/sole practitioner but also harms the reputation of the Cayman Islands as a respected international financial centre.

We identified through our general supervisory engagement that many firms had deficiencies and weaknesses in their BRAs. Undertaking a thematic review assists CARA by providing a fuller overall picture of the quality and effectiveness of BRAs in place across supervised firms. It also helps us to identify where firms would benefit from further support and guidance.

Purpose

The purpose of this thematic review was:

- To ensure all supervised firms had a BRA in place and could produce a current version to CARA;
- To assess and therefore enhance the quality of BRAs conducted by firms;
- To provide insights and benchmarking. By evaluating and comparing performance across firms to achieve continuous improvement in the implementation of BRAs. By sharing findings, supervised firms can see where they stand with their peers;
- To highlight areas of poor practice where firms can improve; and showcasing good practice in conducting a BRA to assist in the implementation of appropriate and effective policies, procedures, and controls;
- To clarify CARA’s expectations of what it considers to be an effective BRA which meets the requirements of the AMLRs; and
- To help firms produce informative BRAs which will assist them in their application of a risk-based approach. BRAs are also an invaluable tool which help inform and support CARA’s understanding of ML/TF/PF risks at the firm level and across the legal sector.

Methodology

This review focused on assessing the soundness of the methodologies applied by firms in undertaking their BRAs. We assessed to what extent firms objectively and fairly rated their inherent ML/TF/PF risks and, where provided, their control effectiveness and residual risks. In doing so CARA considered the information firms had taken into account in carrying out their BRA, the level of quantitative and qualitative data included in the BRA, and evidence provided to support conclusions drawn.

The thematic was a desk-based review of supervised firms’ BRAs, and the findings are based on a representative sample.

¹ AML to be read as also including CFT, CPF and TFS

Sample

At the outset of the thematic review, CARA’s supervised population comprised 53 law firms including sole practitioners.

This review assessed a total sample of 41 BRAs (77% of the supervised population). Most of the BRAs had already been submitted by firms under CARA’s AML Return exercise carried out in May 2021, with the remainder of BRAs provided thereafter upon CARA’s request.

The representative sample comprised BRAs produced by 28 supervised firms and 13 supervised sole practitioners as shown by the graph opposite.

During the preliminary stages of the review, it was noted that 41% of BRAs were dated after CARA’s initial request in May 2021, which suggests that some firms may have not had a BRA in place until prompted by CARA or had updated prior to submitting.

A total of nine firms provided BRAs which were not included in the review due to either a) being a newly established firm at the time; or b) the firm submitted a document that was not a BRA, for example, providing a client onboarding document, a general risk register for the firm, or a client risk assessment template. Three firms failed to submit a BRA entirely.



Firms which fail to have an appropriate BRA in place, or where CARA finds significant delay in implementing a BRA, are referred to enforcement and can result in a sanction.

Regulatory Requirements

Under Regulation 8(1) of the AMLRs, a person carrying out relevant financial business (“RFB”) is required to conduct a BRA appropriate to the nature and size of the business, to identify, assess, and understand the money laundering, terrorism financing and proliferation financing risks in relation to:

- its clients;
- the country or geographic area in which its clients reside or operate;
- its products, services, and transactions; and
- its delivery channels.

In addition, the AMLRs further require that persons carrying out RFB - (a) document their BRA; (b) keep the BRA current; (c) consider all the relevant risk factors before determining the overall level of risk and the appropriate level and type of mitigation to be applied; and (d) provide their BRA to their Supervisor upon request.

In accordance with Regulation 8A of the AMLRs, when assessing the risk of money laundering or terrorist financing in a particular country or geographic area and the extent of measures to manage and mitigate that risk, firms should take account of credible sources related to ML, TF, PF, corruption, and any other criminal activity.

Regulation 9 of the AMLRs requires firms to also identify and assess ML/TF/PF risks that may arise in connection with the development of new products and business practices, new delivery mechanisms and new or developing technologies, and take appropriate measures to manage and mitigate these risks.

A firm’s BRA should identify and assess the inherent ML/TF/PF risks faced by the firm. It may also include the effectiveness of the control environment designed to mitigate those risks and address the need to implement additional measures to manage residual risks, where necessary.

Firms should also refer to Chapter 2 of CARA’s Guidance Notes which provides further details to assist in the implementation of these requirements.

Findings

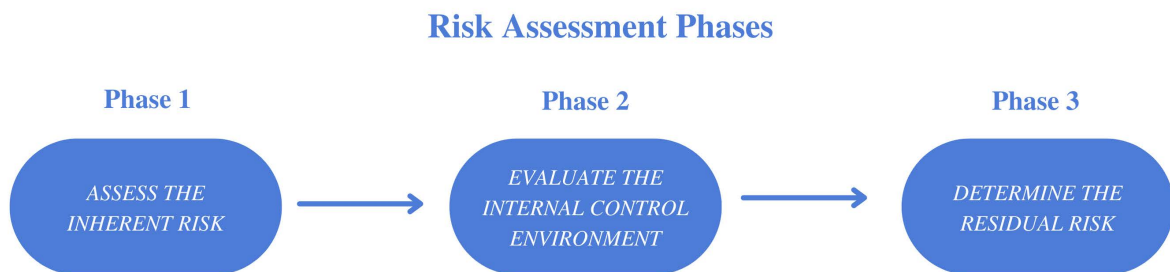
In this review, CARA examined the following aspects:

- A. The extent to which firms understood the concept and importance of establishing **inherent** risk which should result in an objective and comprehensive assessment of the firm’s exposure and vulnerability to ML/TF/PF risks. Where provided in BRAs, we also reviewed how well firms applied appropriate controls, assessed control effectiveness, and calculated **residual** risk;
- B. The soundness of the methodologies adopted by firms in conducting their BRAs.
- C. The level of detail provided in the BRAs and to what extent all relevant risk categories and sub factors had been considered and evaluated;
- D. The firms’ use of both qualitative and quantitative data and evidence provided to support conclusions and risk ratings drawn; and
- E. The governance applied to the BRA including senior management approval, review process, and internal staff awareness.

The findings are detailed in sections A to E, below.

Section A: Understanding Inherent Risk, Mitigating Measures & Controls, and Residual Risk

First and foremost, a BRA should consider all relevant inherent ML/TF/PF risk factors to determine the firm’s inherent risk rating. A BRA may also assess the nature of mitigating controls both from a design and operational effectiveness perspective, to arrive at the firm’s residual risk. The residual risk should be at an acceptable risk level and within the firm’s established risk appetite. The BRA process can be considered in three phases:



Phase 1

The most critical is Phase 1 – Assessing the **Inherent** Risk. A firm cannot design and implement appropriate and effective internal controls if, from the outset, it does not understand and has not identified its exposure and vulnerability to ML/TF/PF risks.

Inherent Risk



Inherent risk is not the same as Actual risk. It is the level of risk that exists before controls, or any mitigating measures, are applied.

Identifying and assessing inherent risk should be the starting point when undertaking a BRA. Put simply, this goes into questioning what might criminals seek to do through the firm; what are the ways in which the firm may be vulnerable to becoming involved in, or otherwise facilitating, ML/TF/PF through its clients, legal services, the way in which its services are provided etc.

In accordance with the AMLRs, firms are required to consider all relevant risk factors before determining the overall inherent risk rating and ensure that this is clearly demonstrated in the BRA. Thus, evidencing the firm

understands and acknowledges its inherent risks. This should be done before detailing any mitigation measures or controls and calculating the residual risk.

Of the 41 BRAs reviewed, 61% referred specifically to inherent risk.

Inherent Risk Assessment Examples	
 <p><u>Good Practice</u> Overall inherent risk rating that is explained well</p>	 <p><u>Poor Practice</u> Assessment of inherent risk that does not consider all relevant risk factors</p>

Phases 2 and 3

Documenting Phases 2 and 3 in a BRA is a matter of preference. Firms may decide to produce a BRA containing an assessment of inherent risk only (Phase 1). However, a firm will still need to evidence to CARA how it meets the requirements of Regulation 8 (b), (e) and (g) of the AMLRs, which includes determining the appropriate level and type of mitigation to be applied to the risks identified, implementing policies, controls, and procedures, and monitoring controls.


Internal Controls

Controls are procedures, systems, and activities put in place to detect and protect against the materialisation of ML/TF/PF risk.

Firms are required to implement policies, controls, and procedures approved by senior management, to manage and mitigate the inherent risks that have been identified by the firm. For the purposes of the BRA, firms should think widely and determine which controls would address each inherent risk factor or vulnerability. Sometimes, it might be one control or a mix of controls that are required.

The assessment of a firm’s internal control environment should consider the design and operating effectiveness of the controls in place i.e., how effectively does the control offset the identified risk. Testing of controls should ideally be carried out by a person or team with a degree of independence from the risk areas and should use proportionate sampling techniques. Control ratings should be categorised to identify a clear bucket for the functionality of the controls such as ‘effective,’ ‘needs improvement,’ ‘weak’ and ‘not tested.’

In this regard, only approximately 10% of BRAs provided an actual rating of effectiveness for the controls in place. In addition, the majority of the BRAs which included a residual risk score did not adequately describe the specific internal controls implemented and/or did not evaluate the quality of the risk controls. Consequently, the determination of residual risk was neither substantiated nor may it have been accurate in those cases.

Case Study 1 – Assessing the Internal Control Environment	
<p>The BRA of a medium-sized international firm outlined its assessment of AML controls across the following areas:</p>	
 <p>Good practice!</p> <ul style="list-style-type: none"> • Corporate Governance • Policies and Procedures • Risk Based Approach • Client Due Diligence • Ongoing Monitoring / Sanctions Screening 	<ul style="list-style-type: none"> • Suspicious Activity Identification and Reporting • Training • Independent Testing and Oversight • Record Keeping and Retention • Other Controls
<p>The assessment of each area was based on control design and operating effectiveness and resulted in ratings of ‘Effective’ or ‘Partially Effective’. This ultimately fed into the firm’s residual risk assessment score.</p>	

Avoid Simply Stating Controls



A large international firm's BRA clearly set out its conclusion on both inherent and residual risk. However, the firm failed to provide an assessment of the effectiveness of its controls and/or identify any gaps or weaknesses. Controls were described in varying levels of detail, referring mostly to general onboarding processes and did not mention specific controls.

To make an accurate determination of the overall residual risk, a firm must assess the effectiveness of its internal controls, not simply describe controls in a general manner, or state the controls that the firm currently has in place without being specific as to the risks mitigated.

CARA would not expect a firm to have effective controls across the board with no issues, deficiencies or weaknesses identified. This would be unusual. Should the BRA highlight controls that are not designed or operating effectively or simply do not exist, this should trigger an action for the firm to remediate this.

Residual Risk

Residual risk is the calculation of risk that remains after controls are applied to the inherent risk. It can be used as an indicator of how well ML/TF/PF risks are being managed by the firm.

The residual risk can be determined by balancing the level of inherent risk with the overall strength of effectiveness of the risk mitigation measures and controls. To effectively lower a firm's residual risk, the inherent risk level should be reduced, or the internal controls should be strengthened. For example, a strong internal control environment could result in a lower residual risk rating in comparison to the inherent risk rating.

In this regard, the majority of BRAs (83%) included an assessment of residual risk. It was observed, however, in a significant number of cases that it was not possible to understand or verify the level of residual risk due to the following reasons:

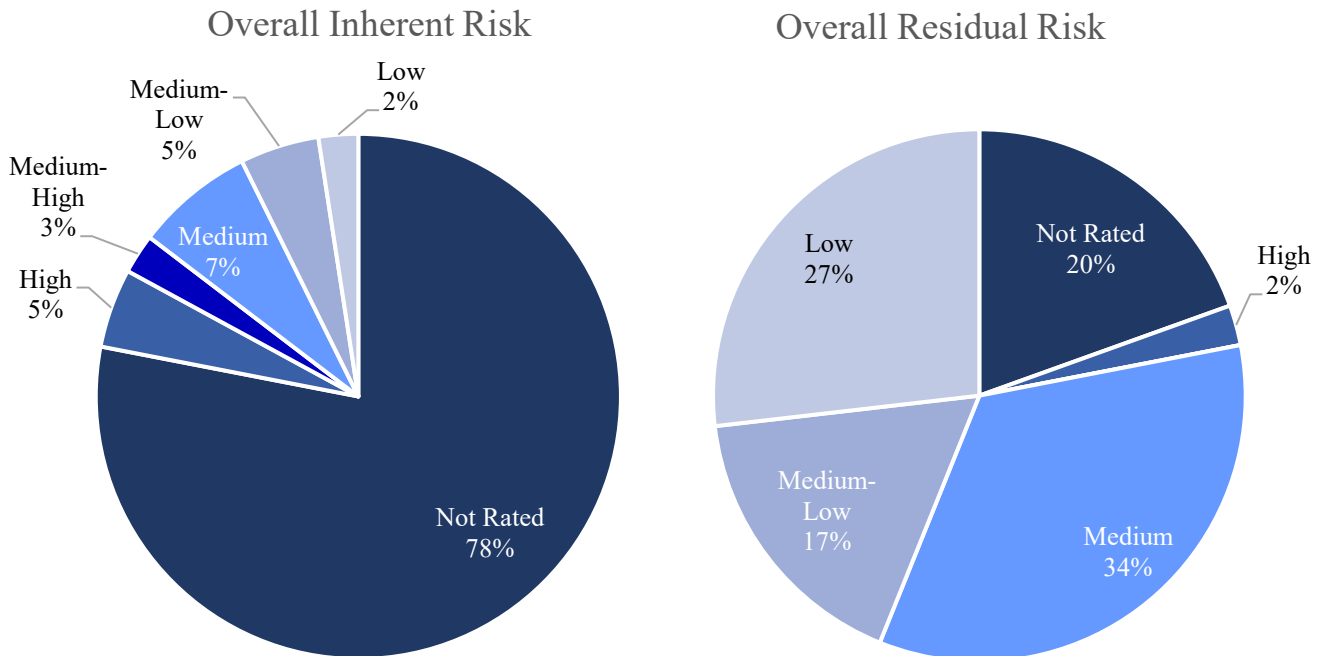
- No assessment of the internal control environment had been conducted.
- The BRA did not provide control scores/ratings.
- The control risk score did not justify the residual risk rating.
- The BRA did not refer to the firm's specific controls and simply listed generic controls as examples.

Determination of Overall Inherent Risk and Residual Risk

BRAs should document a clear overall conclusion and final rating of firms' ML/TF/PF risks. This may be from an inherent risk only or both inherent and residual risk standpoint, depending on the methodology applied. There is no defined method in how overall inherent risk should be calculated. The conclusion drawn is a matter of judgement and should reflect all key areas of risk such as the nature of the RFB services being provided and the client base. Calculation of residual risk, on the other hand, is the inherent risk rating less the control risk rating to provide a residual rating/score.

This review identified that firms had varied approaches in how they rated levels of risk in their BRAs, with some using a three-tier basis such as low, medium, and high risk and others adopting a more granular scale using a five-tier basis.

Below is a breakdown of how the BRAs concluded on firms' overall level of ML/TF/PF risk exposure. It was noted that not all 41 firms rated both their overall inherent and residual risks, with some firms rating either overall inherent risk or overall residual risk and others did not provide any overall ratings at all. Approximately 10% of BRAs did not provide any overall conclusion on the level of risk (i.e., neither inherent nor residual).



Despite 78% of BRAs failing to provide an overall inherent risk rating, it was noted that most BRAs documented an inherent risk rating against each of the relevant risk categories (explored in more detail in Section C below) and were just short of concluding on the overall level of inherent risk exposure.

Of the very few BRAs which provided overall ratings for both inherent and residual risk, 60% reported no difference between the inherent and the residual risk level. The remainder reported a residual risk rating lower than the inherent risk rating. However, in these instances the residual risk ratings could not be substantiated owing to the fact the BRA either did not document the internal control testing results or documented an internal control score that was less than effective.

Section B: Business Risk Assessment Methodology

The design and application of an appropriate BRA methodology is key to identifying the overall ML/TF/PF risk exposure to a firm.

In this review, it was noted the BRAs varied considerably in length, format, and structure. Smaller firms engaged in RFB matters on an occasional and or infrequent basis documented shorter and more concise BRAs. At the other end of the scale, some of the BRAs of larger international firms with a higher volume and wider range of RFB matters were more detailed analysing likelihood and impact, financial crime risk scenarios, and included risk matrices.

CARA recognises there are many methods and formats for conducting a BRA and does not therefore provide a BRA template. A firm should decide how best to carry out its BRA. The methodology may be quite simple or more sophisticated employing advanced techniques, depending on the nature and size of the firm and the range and extent of its legal services and client base. Whatever methodology is adopted it should be relevant, consistently applied, and easily understood.

Bearing in mind that firms are required to conduct a BRA appropriate to the nature and size of their practice, it is good practice to provide a brief description of the firm. In this regard, 66% of BRAs provided a general overview

of the firm in the introduction, including key information such as, but not limited to: governance, number of partners/staff, description of relevant financial business offered, and types of clients represented.

After providing a general background and overview of the firm, it is important the BRA then fully describes the methodology applied to enable CARA to understand how ratings and conclusions were reached.

BRA Methodology – Good Practices Observed



Good practice!

- ✓ Describing the sources of data and information which were considered.
- ✓ Stating the period of data analysed.
- ✓ Providing a description of the procedures for testing effectiveness of controls.
- ✓ Referencing the extent to which the AMLCO, MLRO, other compliance staff, senior management, audit, and any other relevant parties (including outsourced agents) have been involved in the risk assessment process.
- ✓ Describing the procedures for monitoring and timely updating of the BRA to ensure its accuracy.

Rating/Scoring

There is no one-size-fits-all calculation of risk scores. Firms should make their own determination of appropriate risk scores and weightings to be assigned to risk categories and sub risk factors. The methodology should include detailed rationale for the principles applied. The key is that the BRA methodology is logical, comprehensible, and can be replicated as and when the risk assessment is updated.

A BRA will never result in zero risks. On the other hand, a BRA which determines a high level of inherent risk should not be perceived negatively or in a way that suggests a firm ought to consider de-risking (avoiding risk). A firm can provide legal services which have a higher inherent risk. What is important is the firm is fully aware of the risk exposure, has appropriate mitigating control measures in place, and it is within the firm's risk appetite.

Although limited, CARA noted instances where the methodology behind a firm's BRA resulted in understated overall ML/TF/PF risk exposure. This may have been due to a bias towards more lenient risk ratings, or the application of inappropriate weightings to individual risk factors, or combination of factors. A firm should ensure its risk methodology and tools appropriately capture and assess its ML/TF/PF risks.

Case Study 2 – Be Cautious of Rating Bias



A domestic firm's BRA matrix outlined the relevant risk areas and corresponding risk factors. Each risk factor was assigned a numerical risk score that ultimately fed into an overall residual risk score. There were 10 risk factors in total, with each having equal weightings and these were rated as follows: 2 factors scored High risk, 4 scored Medium, and 4 scored Low. The overall risk rating was calculated as Low.

Based on the scoring method, the overall risk rating would elevate to Medium if the following were to occur:

- a) A low risk factor was to change to High risk, which would add 4 points to the score, or
- b) Two Medium risk factors were to change to High risk adding 2 points each to the score.

This particular case displays a lenience towards a lower risk rating.

Examples of flawed methodologies include cases where:

- The residual risk rating is determined to be Medium when inherent risk was rated High and control effectiveness deemed to be deficient.
- The overall inherent risk score is rated Low despite the majority of the inherent risk factors being rated as either Medium or High.
- The risk weightings calculations make it difficult to achieve a high-risk rating.
- The risk factor assessed is not directly linked to ML/TF/PF vulnerabilities.

National and Sectoral Risk Assessments

A firm must have regard to the most recent version of the NRA, the Legal Sector Risk Assessment, and any other relevant sectoral risk assessments, when creating and maintaining its BRA. The BRA should be aligned to the findings in the national and sectoral risk assessments. Any differences or deviations must be fully explained and evidenced in the BRA.

In this regard, it was identified that 39% of BRAs drew conclusions that were not aligned to the findings of the NRA, 2015 (in place at the time) and did not provide any justification for the variances.

Case Study 3 – Documenting Rationale



Good practice!

In the assessment of legal services risk, an international firm considered its shipping work to be low-medium risk.

The firm’s assessment was not aligned with the Legal Sector Risk Assessment which rates shipping as higher risk. However, the BRA acknowledged this exception and documented its rationale for having a reduced risk rating.

TF/PF Consideration

Most importantly, firms must also ensure their methodology includes undertaking an assessment of both TF and PF risks and documents how the TF and PF risks may impact the firm. Firms should consider the TF NRA and the PF Assessment in identifying and drawing conclusions in respect of TF and PF risk exposures.

The majority of BRAs reviewed failed to provide an assessment of firms’ risks pertaining to TF/PF, with only (49%) referring to TF and (41%) to PF. The BRAs which did mention TF and PF tended to simply reference the TF NRA and PF Assessment but did not carry out a detailed assessment of how the firm itself may be vulnerable in these areas.

It was also observed, BRAs either grouped TF/PF in with ML risk or grouped TF and PF together. The risk exposures for TF, PF, and ML are different and should be considered separately.

Section C: Comprehensive Assessment of Relevant Risk Categories

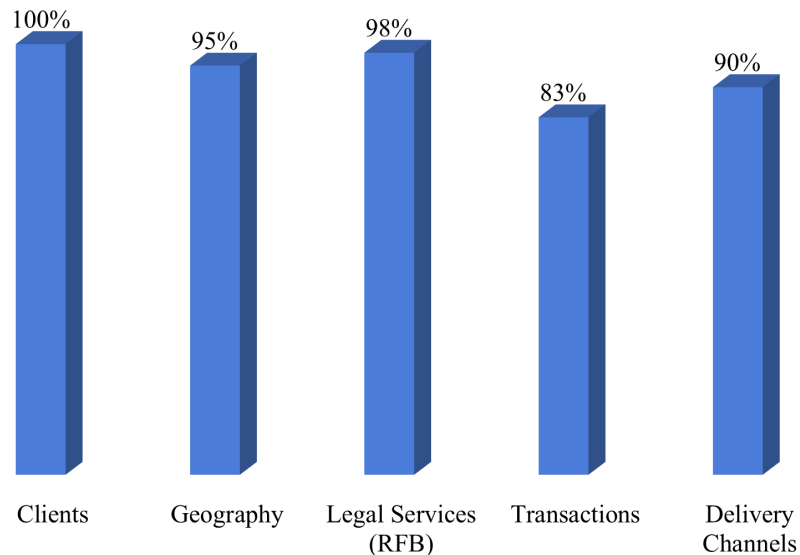
A BRA should be comprehensive in identifying and assessing the firm’s ML/TF/PF risks. In accordance with the AMLRs, a firm should consider its ML, TF, and PF risks with respect to the below five risk categories. For each category, a BRA should include the underlying risk factors which were considered.



Nearly a fifth (17%) of BRAs failed to demonstrate that all five relevant risk categories were considered. It was apparent that some BRAs reflected only the risk categories/factors that the firms felt affected their practice the most and, as a result, did not include an assessment of all the relevant risk categories.

As shown in the graph below, all BRAs considered client risk but only 83% considered transaction risks. Ten percent (10%) of BRAs failed to assess delivery channel risk and 5% failed to consider geographical risk exposures. However, even when risk categories were considered, it was found that most BRAs lacked sufficient detail in assessing underlying risk factors which resulted in an overall weaker analysis.

RELEVANT RISK CATEGORIES CONSIDERED



Although limited, there were three instances in which the BRAs reviewed highlighted general ML risk factors and did not provide any specific information to evidence these were vulnerabilities faced by the firm.

When comparing the content of all BRAs with registration, AML Return data, supervisory engagement records held by CARA, and with the firms' own websites, it was apparent that a significant minority of BRAs did not match the type and volume of RFB client matters previously reported and the legal services being provided by the firm.

The next section explores the findings for each risk category in more detail.

Client Risk

Client risk considers the vulnerability that clients or those acting on behalf of another person or entity, may be involved in ML/TF/PF activities. All firms considered their client risk to some extent in the BRAs. It was noted, however, that whilst most BRAs identified and evaluated client risk factors, the majority lacked a comprehensive analysis of risk in this area. Some BRAs failed to highlight key risk factors that may be relevant to the firm's client base, such as HNWI and clients operating in higher risk sectors, and in some instances, the client base assessment provided was insufficient given the size and nature of the business.

Key Client Risk Factors:

- **Client types** – Only 22% of BRAs considered the composition of client base in terms of natural and legal persons. Not all BRAs (58%) detailed whether the firms' clients were domestic or foreign clients. There was also a lack of analysis of ownership and control structure of clients which were legal persons.
- **PEPs** – Nearly a third of BRAs (29%) did not detail whether they had considered PEP relationships and relatives/close associates.
- **HNWIs and UHNWIs** – Only 10% of BRAs demonstrated a consideration and identification of the risks associated with HNWIs and UHNWIs.
- **Clients in higher risk sectors/industries** – Nearly two thirds (63%) of BRAs did not consider clients operating in higher risk sectors/industries such as shipping, money services business and NPOs/charities for example.

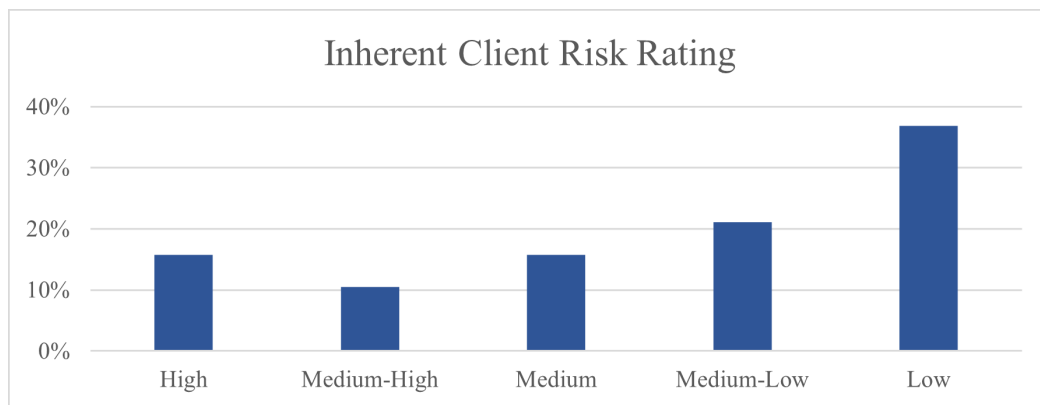
Several BRAs provided a breakdown of and/or highlighted the assigned risk ratings of the firms' clients/ client matters and used this as a factor in assessing their inherent client risk analysis. This provided a good snapshot of the firm's overall inherent risks pertaining to its clients.

Client Risk Analysis – Good Practices Observed



- ✓ Including a detailed breakdown of clients by high-risk industries, for example extractive industries, energy, virtual assets, and real estate
- ✓ A separate and focused analysis on PEPs within the firm, differentiating between foreign and domestic PEPs
- ✓ Inclusion of PEP associates and family members
- ✓ Stating total number of RFB clients and RFB client matters in which the firm acted
- ✓ Providing a breakdown of RFB clients by their assigned risk rating
- ✓ Identification of HNWI and UHNWIs
- ✓ Identification of sanctioned persons/entities
- ✓ Maturity of client base

Based upon the overall inherent risk rating for Client Risk (where provided in the BRAs) it was observed that 58% of firms considered their practice to be less susceptible to ML/TF/PF risks through their clients, rating the overall risk exposure either low or medium low². These firms were mainly domestic firms, with three being international firms.



Geographical Risk

Ninety-five (95%) of BRAs provided an analysis of the risks posed by the countries or geographic areas in which their clients reside and or operate.

Thirty nine percent (39%) of BRAs referred to high-risk jurisdictions and highlighted the proportion of the firms' client base that resided and or operated in these jurisdictions.

It was noted some BRAs simply stated that the majority of the firms' clients were from 'low-risk jurisdictions' and did not categorize the remaining minority of the client base or identify the jurisdictions in which clients resided/operated.

Several instances were identified in which the BRA failed to identify high risk jurisdictions. Countries that are known to present higher ML/TF/PF risks were considered to be low risk in the BRA. Firms should refer to Regulation 8A (2) of the AMLRs that lists the factors in which countries or geographic areas should not be assessed as having a low risk of ML/TF/PF.

A number of BRAs detailed reliance on internal outdated lists, which were not updated periodically. Firms should conduct their own country risk assessments and document a list of high-risk jurisdictions. This list should consider credible sources as per Regulation 8A of the AMLRs and be reviewed frequently.

The BRA should provide a geographic footprint of the firm's operations (both domestic and international) and its clients. Below is a non-exhaustive list of notable factors that firms should consider when assessing geographical risks:

² With the caveat that not all BRAs provided an inherent risk rating for the category of client risk.

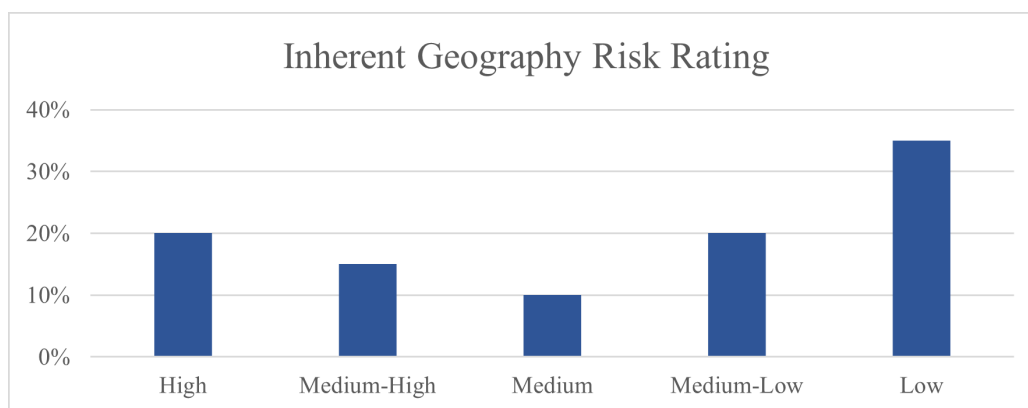
- Jurisdictions in which clients (and beneficial owners) are based
- Location of business operations
- Origin and destination of transactions
- Association with high-risk jurisdictions
- Designated Persons and sanctioned regimes.

Geographical Risk Analysis – Good Practices Observed



- ✓ Appendices that include a list of jurisdictions identified as having a higher risk of ML/TF/PF by credible sources such as FATF, IMF, World Bank, the OECD, and the UN.
- ✓ Consideration of jurisdictions with significant levels of corruption as identified by Transparency International
- ✓ Analysis of client base by country

Based upon the overall inherent risk rating for Geographical Risk (where provided in the BRAs), it was observed that the level of identified risk varied considerably across firms³. This may in part be due to the manner in which firms assessed this risk exposure.



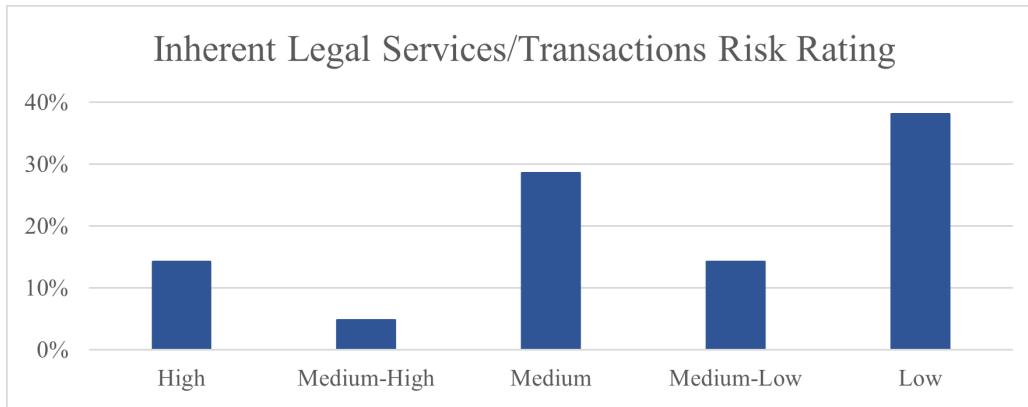
Legal Services and Transactions Risk

For the purposes of the BRA, a firm should assess what proportion of its practice relates to RFB activities, especially RFB activities identified as higher risk by the NRA and Legal Sector Risk Assessment.

Nearly all (98%) of BRAs included an assessment of the firm’s legal services risks and a lesser amount (83%) included an assessment of transactions risk. It was noted that some BRAs tended to document what the firm does not do rather than focus on assessing the risks associated with the type of work the firm does provide.

Despite BRAs highlighting both firms’ provision of advisory services to legal persons and arrangements and conveyancing work as being inherently higher risk activities, more than half of BRAs concluded the overall inherent risk for legal services and transactions to be either Low or Medium-Low.

³ With the caveat that not all BRAs provided an inherent risk rating for the category of geographical risk.



With respect to transactions risk, most BRAs identified the risks associated with client accounts and the potential for misuse. BRAs also noted the risks surrounding cash acceptance and whether cash payments were accepted in the day-to-day operations.

Below is a non-exhaustive list of notable factors that firms should consider when assessing the ML/TF/PF risks posed by legal services and transactions:

- Nature, complexity, and diversity of legal services;
- Legal services that may attract a higher level of ML/TF/PF risks such as high value conveyancing, advising on the creation of legal persons and arrangements and trust services;
- Proportion of clients provided with higher risk legal services;
- Level of transparency that the legal service or transaction affords;
- Involvement with crypto assets and virtual asset services providers;
- Receiving unsolicited payments; and
- Legal services offered outside of the firm’s main practice areas/ area of expertise.

Legal Services and Transactions Risk Analysis – Good Practices Observed



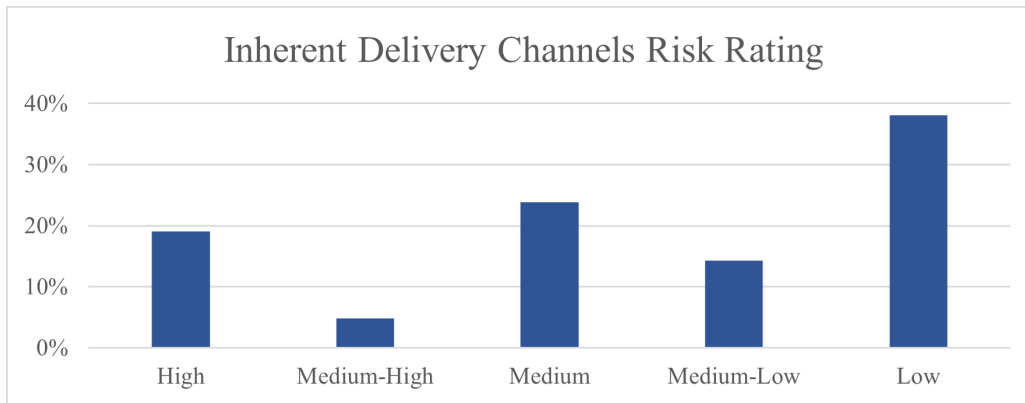
- ✓ Highlighting the specific RFB services offered by the firm
- ✓ Analysis of legal services that present the greatest ML/TF/PF risks
- ✓ Percentage of clients involved in higher-risk service offerings
- ✓ Firm’s susceptibility to the misuse of client account
- ✓ Volume, value, and percentage of transactions involving cash payments
- ✓ Involvement with crypto assets and virtual asset providers

Delivery Channels Risk

The majority (90%) of BRAs included delivery channels as a risk factor. Most BRAs identified the method by which clients obtained legal services, such as face-to-face, through intermediaries or on a non-face-to-face basis. However, the details of these delivery channels were rarely evaluated (i.e., quantitative data), resulting in an overall lack of depth of analysis in this area.

In assessing the inherent risk posed by delivery channels, this review noted a variety of risk ratings documented in the BRAs. Seventy-six percent (76%) of firms that assigned an overall inherent risk rating in this area considered the risk exposure ranged from Medium to Low⁴. The remaining firms considered this to be a higher risk area due to the significant portion of business conducted through intermediaries.

⁴ With the caveat that not all BRAs provided an inherent risk rating for the category of delivery channels risk.



Firms should detail the features of delivery channels used, which may include the ability to reliably identify/verify clients through remote or digital onboarding, products or services delivered by post, telephone, internet etc. or the use of introducers or intermediaries (and the nature of their relationship with the firm). Below is a non-exhaustive list of notable factors that firms should consider when assessing the ML/TF/PF risks posed by its delivery channels:

- Number of transactions for each delivery channel
- Number of matters that rely on indirect contact with clients rather than a direct relationship
- Analysis of the business conducted on a non-face-to-face basis
- Work undertaken through intermediaries or other third parties

Delivery Channels Risk Analysis – Good Practices Observed

Good practice!

- ✓ Breakdown of percentage of business conducted per delivery channel
- ✓ Assessment of the proportion of unsolicited work
- ✓ Percentage of business derived from referrals

Section D: Adequate Quantitative Data

BRAs should include both qualitative and quantitative data analysis to demonstrate the firm has a good grasp of its exposure to ML/TF/PF risks. Firms should seek to support and substantiate assertions in the BRA as much as possible with hard data that is verifiable and replicable and with factual evidence.

A quantitative analysis can assist in the firm’s evaluation of the relevant risk categories, more accurately reflect financial crime risk exposure, and draw attention to the areas that present greater risk.

In this regard, it was noted the use of quantitative analysis in the BRAs was very limited. Only 5% of BRAs included sufficient quantitative analysis that was in line with the size and nature of the firm’s business. Relying primarily on qualitative analysis, with limited to no quantitative analysis, may potentially impede the ability to have an in-depth understanding of the ML/TF/PF risks. It is acknowledged that some firms may have used quantitative analysis to arrive at the conclusions stated, however, this should be documented in the BRA.

There were some instances where quantitative data was included but did not align with the conclusions provided. For example, a BRA reported a high number of high-risk clients, however the firm’s overall inherent client risk rating was determined to be low. Quantitative data should complement the conclusions drawn.

The BRA should quantify in measurable terms a firm’s clients, legal services, and delivery channels etc. As far as possible, BRAs should avoid qualitative descriptive terms such as ‘most’, ‘some’ and ‘majority’ and instead provide accurate figures, reliable percentages, or figure estimates. CARA encourages firms to leverage their annual AML Return data as a starting point to enhance their BRAs.

Of the few firms that were considered to have a sufficient quantitative analysis, an effective use of quantitative metrics was displayed in the BRAs and demonstrated a more in-depth understanding of the ML/TF/PF risks. Below are examples of quantitative data used in the BRAs:

- Number and percentage of clients who are PEPs
- Number and percentage of high-risk clients
- Breakdown of client risk rating per RFB clients
- Number and percentage of conveyancing matters
- Amount of business that is domestic and cross-border
- Number of clients introduced by intermediaries and third parties
- Number of SARs

Case Study 4 – Good Use of Quantitative Data



Good practice!

In this example of good practice, a small sized firm displayed a good use of quantitative data in its BRA. The BRA differentiated between its total clients and RFB clients. The firm's analysis of RFB client risk identified 5 PEP clients, and 6 clients by high-risk industries, namely shipping and state-owned entities.

The BRA also provided a jurisdictional breakdown of all RFB clients.

Section E: Governance

Firms should have documented processes for conducting their BRAs that outline the methodology, application of the BRA, and provide an audit trail for the ongoing review process.

The BRA and any supporting documentation should also be easily accessible and readily available upon CARA's request.

Key observations in this review regarding the format, structure, and application of the BRAs are detailed below.

- **A stand-alone document** – The BRA should be presented in a written stand-alone document (in paper or electronic form) that is readily accessible. In this regard, the majority of the BRAs were documented separately to the firms' AML manuals.
- **Date of assessment** – Twenty seven percent (27%) of BRAs did not include the date or period in which the assessment took place. Only 12% of BRAs were version controlled. Firms should retain all previous versions of the BRA to evidence continuous compliance.
- **Author** – Less than half (41%) of BRAs stated the author of the BRA or the person responsible for reviewing and monitoring the document.
- **Outsourcing** – It was observed that a limited number of firms involved an external agent to assist in the preparation of the BRA. In these cases, it was evident a template had been used. Whilst templates can be helpful, it was found that these BRAs were lower in quality, tended to be generic, and not tailored to the firm.
- **Senior management approval** – Over a third (39%) of BRAs failed to evidence senior management buy-in or approval. The BRA should be challenged and signed off by senior management.

Research shows that involvement of senior management in the BRA process “results in a higher quality risk assessment and means that the risk assessment holds greater weight within the firm”.⁵ In large firms, the AMLCO should seek approval for risk assessments and decisions made to ensure the Board/ExCo understand the ML/TF/PF risks the firm faces and risk tolerance thresholds are not exceeded.

- **Risk appetite/Risk tolerance** – It was observed that several firms, mostly larger international firms, included a statement on the firm's risk appetite and risk tolerance level in their BRAs, but this was not universal.

⁵ FCA, UK

- **Review process** – BRAs should evolve and are not static documents. Just over half (51%) of BRAs failed to demonstrate that the firm had a mechanism in place to conduct regular reviews of its BRA. In some cases, the next review due date was not stated and in other cases, it was not possible to determine the last review date.

Firms should undertake periodic reviews to maintain the relevancy and accuracy of the BRA. Timeframes should be documented for regular updates as well as detailing trigger events that may result in an earlier review. A trigger event could include changes in legislation, firm acquisition/merger, providing a new legal service or other material changes in the firm's ML/TF/PF risk exposure, a new criminal typology or trend. Depending on the circumstances, it may be necessary to update the entire BRA or only the parts of it for with the level of risk may have increased/decreased significantly.

- **Staff Awareness** – A firm should be able to communicate its BRA easily across its organisation (i.e., it should be in a clear format which is easy to follow and understand). Very few BRAs referred to internal distribution of the document and raising staff awareness of the firm's inherent ML/TF/PF risks.

Conclusion

As this report has detailed, the BRA forms the cornerstone of a firm's AML/CFT/PF risk management. A robust BRA enables firms to better understand their ML/TF/PF risks, implement appropriate policies and control procedures to effectively manage and mitigate these risks, and optimize the allocation of the firms' finite AML/CFT/CPF resources.

Overall, this thematic review has identified attorney-at law firms and sole practitioners need to improve upon the design of BRA methodologies, the effectiveness of BRA implementation, and the rigor of senior management oversight of BRA processes.

Notwithstanding the good practice demonstrated in this review, there are several areas where firms would benefit from making improvements. These are as follows –

- **Assessing inherent risk**
All BRAs must include an assessment of inherent risk. This assessment is twofold. Firstly, BRAs should assess and determine inherent risk ratings for each of the five risk categories – clients, legal services, transactions, geography, and delivery channels. Secondly, BRAs should conclude with a final risk rating of the firm's overall inherent risk (taking into account all five key risk categories) and provide a rationale.
- **Documenting and applying an appropriate methodology**
All BRAs should detail the methodology applied. The methodology should be relevant, consistently applied, and easily understood. Care should be taken with risk scoring and weightings.
- **Assessing both PF and TF risks in addition to ML risks**
It is a requirement of the AMLRs that the firms understand, assess, and evaluate the risks from both TF and PF.
- **Ensuring controls are tested for effectiveness**
A BRA should describe the control(s) which addresses a specific risk identified. All controls should be tested for effectiveness.
- **Providing sufficient quantitative data to support conclusions drawn**
The assessment of inherent risk should be a predominantly quantitative exercise driven by data available within the firm. It is not necessary to apply overly complicated risk rating matrices. Where matrices are utilised within BRAs, the supporting underlying data should also be made available.
- **Determining overall inherent and residual risk**
BRAs should document a clear overall conclusion and rating of the firms' ML/TF/PF risks. This may

be from an inherent risk only or both inherent and residual risk standpoint, depending on the methodology applied.

- **Implementing good governance such as senior management oversight and review processes**
A BRA should be a stand-alone document which is dated, version controlled and easily accessible. It should be challenged and signed off by senior management, a process for regular review should be applied, and the document should be circulated across the firm and feed into the staff training and awareness programme.

Next Steps

All supervised firms should use this report to determine whether their BRA is fit for purpose, meeting CARA's expectations of an organized and informative BRA, and the standards required by the AMLRs.

All BRAs should be able to demonstrate that the firm has identified and assessed its ML/TF/PF risks fairly, objectively, and in a comprehensive manner.

CARA expects to see an overall improvement in the quality of BRAs following the publication of this report. All supervised firms are on notice that BRAs will be required to be submitted in the next AML Return exercise to be rolled out in early 2023.

Supervised firms can look forward to an upcoming outreach session specifically covering this thematic review.

CARA will continue to engage with firms to promote best practices and maintain high AML/CFT/CPF standards within the legal profession.