Guernsey Financial Services Commission

Money Laundering and Terrorist Financing Business Risk Assessments

Thematic Review - 2022

Executive summary

In 2022 the Commission conducted a thematic review to assess how well firms identify and assess the money laundering and terrorist financing risks to their business and apply the appropriate level of controls to mitigate those risks (the "thematic").

We reviewed the money laundering and terrorist financing business risk assessments from 104 firms from across the Bailiwick's financial and professional services sectors to establish the extent to which the money laundering and terrorist financing risks identified in the Bailiwick's National Risk Assessment had been taken into account, to gauge whether the regulatory changes to these assessments brought about in 2019 had been met, and to assist the Commission's understanding of the risks which firms' are currently identifying as key threats to their business.

The results from the thematic are positive, most of the business risk assessments we reviewed drew upon the findings from the National Risk Assessment and met the regulatory requirements with many points of good practice noted. Whilst foreign predicate offences of fraud including tax crimes, bribery and corruption continued to be identified as the main money laundering and terrorist financing threats to Bailiwick firms, which is consistent with the National Risk Assessment's findings, many firms had identified sanctions evasion risk within business risk assessments that were drawn up in advance of the UK's imposition of Russian sanctions for its invasion of Ukraine. Firms also commonly identified falling victim to fraud due to the evolving threat of cybercrime.

In total seven areas for improvement were identified with the two key areas for improvement, based on the prevalence of the issues identified throughout the sample, being:

1. firms could benefit from additional research and using the National Risk Assessment to help them improve upon identifying the TF risks which are relevant to their businesses. Firms are encouraged to revisit where their terrorist financing vulnerabilities exist across their customers; jurisdictions; products; services; transactions and delivery channels; and
2. firms would be well advised to make more use of their management information in their money laundering and terrorist finance assessments to ensure that those assessments are relevant and tailored to the business, rather than generic. For licence or registration applicants they are encouraged to draw upon the data and information they have used in their business plans and forecasts.

We hope that the case studies, good practice points and areas for improvement in this report will assist firms in assessing their money laundering and terrorist financing risks and developing commensurate policies, procedures and controls for mitigating those risks. I would like to take the opportunity to thank the firms involved in participating in the completion of this thematic.

Fiona Crocker
15 December 2022

Summary of areas for improvement

TF risk understanding *(page 19)*	**Issue:** we noted that the terrorist financing risk assessments were less developed compared to money laundering risk assessments. **Action:** firms could benefit from additional research and using the National Risk Assessment to help them improve upon identifying the TF risks which are relevant to their business. Firms are encouraged to revisit where their terrorist financing vulnerabilities exist from their customers; jurisdictions; products; services; transactions and delivery channels.
Tailoring to specific risks *(page 14)*	**Issue:** we noted a common theme among firms that greater use could be made in their money laundering and terrorist financing business risk assessments of their management information about customers, jurisdictions; products; services; transactions and delivery channels, which would make their assessments more relvant to their business. **Action:** firms should consider where they can enhance their money laundering and terrorist financing business risk assessments through increased use of management information about their customers, jurisdictions; products; services; transactions and delivery channels and the nature of the underlying predicate offences in suspicious activity reports.
Transactions *(page 16)*	**Issue:** we noted that where firms are involved in the inward and outward flow of cross-border funds, not all were considering their management information on geographic origin and destination of these flows which also takes into account whether the flows are connected with countries listed on Appendices H and I of the Handbook. **Action:** firms involved in the receipt and/or payment of funds across jurisdictions should consider including management information covering this information and consider the money laundering and terrorist financing risks associated with the jurisdictions identified.
Delivery channels *(page 16)*	**Issue:** we noted that firms tended to give insufficient consideration to their money laundering and terrorist financing risks in connection to their delivery channels, i.e. introducer, intermediary, non-face-to-face customers, outsourced relationships or reliance on independent financial advisers for the delivery of their products and services. **Action:** firms should consider, and where appropriate, develop their analysis of their money laundering and terrorist financing risks arising from their delivery channels.
Effective annual reviews *(page 20)*	**Issue:** we noted that some money laundering and terrorist financing business risk assessments contained reference to out of date regulatory provisions such as the Business from Sensitive Sources Notices and the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations 2007. **Action:** firms should ensure that the annual reviews of their business risk assessments identify where updates are required, including out of date regulatory provisions as well as any emerging risks from new products or use of technology.
Overall level of ML and TF risks *(page 10)*	**Issue:** we identified that not all firms provided a summary describing their overall level of exposure to money laundering and terrorist financing risks with an accompanying rationale as to the basis of their conclusions in this respect. **Action:** firms should ensure that they summarise their overall level of exposure to both money laundering and terrorist financing, which includes the rationale upon which their conclusions on overall risk were based.
Accessibility *(page 23)*	**Issue:** we noted that firms adopted a variety of formats and practices to document their money laundering and terrorist financing risks including use of multiple documents, spreadsheets, acronyms and compliance jargon. Some business risk assessments were very lengthy, however the lengthier the assessment the less accessible the key money laundering and terrorist financing risks were. These factors can negatively impact on the audiences' understanding of the key risks. **Action:** firms should be mindful of the overall effectiveness of their documentation by paying particular attention to factors such as the format, length, use of multiple documents, acronyms, compliance jargon when approving the final versions of their money laundering and terrorist financing risk assessments.

Glossary of terms

AML/CFT – Anti-Money Laundering and Countering the Financing of Terrorism

Bailiwick – Bailiwick of Guernsey

Board – Board of directors (or the senior management where it is not a body corporate)

BRA – Business Risk Assessment

Commission – Guernsey Financial Services Commission

FATF – Financial Action Task Force

FCRR – Commission's annual Financial Crime Risk Return

Firm – A financial services or prescribed business subject to the requirements of Schedule 3 and the Handbook

TF – Terrorist Financing

Handbook – The Handbook on Countering Financial Crime and Terrorist Financing

MI – Management Information

ML – Money Laundering

NRA – National Risk Assessment of ML and TF

PEP – Politically Exposed Person

Schedule 3 – Schedule 3 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999

The thematic – Money Laundering and Terrorist Financing Business Risk Assessments Thematic Review

UK – United Kingdom

Contents

Section 1: Background

1.1 Rationale for the thematic

The financial and professional service sectors have had to identify their money laundering ("ML") and terrorist financing ("TF") risks and document those risks and commensurate controls in a Business Risk Assessment ("BRA") since 2007. Such an assessment should form the cornerstone of a firm's anti-money laundering/countering the financing of terrorism ("AML/CFT") framework. As the BRA is such an important document, the Commission has paid considerable attention to these assessments in its AML/CFT supervision since the inception of these requirements.

During this 15-year period we have observed substantial improvements in these assessments. Generally, firms have been good at identifying their ML risks and articulating their controls, but less so at identifying and assessing their TF risks. We have also observed that some firms produce overly generic assessments not tailored to their business.

A variety of groups are regarded as terrorist organisations by most Western democracies. Considerable international attention now attaches to how such groups are funded, including what role international finance centres might play in funding foreign terrorist organisations.

In addition to the increased focus on TF globally, MONEYVAL, during its evaluation of the Bailiwick's compliance with FATF Recommendations in 2014, reviewed the BRAs of the firms it interviewed. On the subject of risk appetite statements, MONEYVAL noted that, "only few statements clearly defined where the financial institution would find it appropriate, based on an assessment of risk, to reject or terminate a business relationship".

In response to the increased focus on TF globally, the role international finance centres could play in funding terror and MONEYVAL's feedback, enhancements were made to the Bailiwick's regulatory requirements for undertaking these assessments. The changes included requiring firms to undertake distinct assessments of both their ML and TF risks, and to separately determine their ML and TF risk appetites.

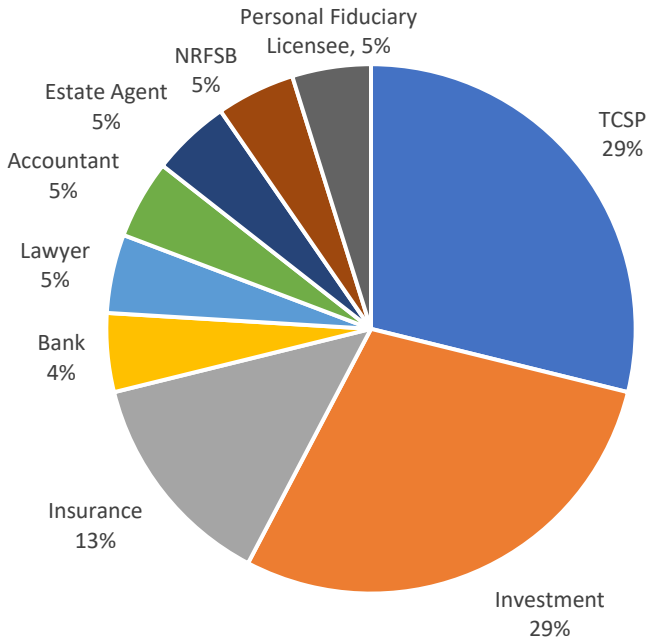
Those changes, which came into effect in March 2019, also required firms to have regard to the National Risk Assessment ("NRA"). The Bailiwick's first NRA was published in January 2020. Allowing for a transitional period, the thematic was undertaken to see how firms responded to the changes and to gauge how much more mature and thorough these assessments have become.

1.2 Purpose of the thematic

The objective of the thematic was to determine the extent to which firms appropriately identified the risks of ML and TF specific to their business by considering the types of customers they have, the jurisdictions their business is connected to, the products and services they offer and the transactions and delivery channels for those products and services. We also considered how well these risks were articulated in their BRAs and the extent to which firms had identified appropriate controls to manage and mitigate the identified risks.

1.3 Scope of the thematic

The thematic comprised a review of the ML and TF BRAs of just over one hundred firms from across all sectors of the Bailiwick's financial services industry namely: banking; trust and company services providers; investment; insurance; lawyers; accountants; estate agents; non-regulated financial services business and personal fiduciary licensees (collectively referenced to as "firms" throughout this report). The number of firms selected from each sector was weighted in proportion to the size and risks associated to each by the Bailiwick's NRA, but we also specifically included in our sample firms which did not attend our 2020 workshops on the NRA. The chart below shows the percentage of firms selected by sector.



Participating firms were required to complete a questionnaire on the topic of BRAs and submit their current ML and TF BRAs.

Section 2: Regulatory requirements

The regulatory requirements in respect of the ML and TF BRAs are set out within Paragraph 3 of Schedule 3 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law 1999, as amended and the rules within chapter 3 sections 3.6 to 3.12 of the Handbook. Paragraph 3 of Schedule 3 provides that:

*"**3. (1)** Without prejudice to the generality of the duty under paragraph 2, a specified business must –*

(a) carry out and document a suitable and sufficient money laundering business risk assessment, and a suitable and sufficient terrorist financing business risk assessment, which are specific to the specified business, and

(b) regularly review its business risk assessments, at a minimum annually and more frequently when changes to the business of the specified business occur, so as to keep them up to date and, where, as a result of that review, changes to the business risk assessments are required, it must make those changes.

(2) In carrying out its business risk assessments under subparagraph (1) the business must consider all relevant risk factors before determining –

(a) the level of overall risk to the business,

(b) the type and extent of the risks that the business is willing to accept in order to achieve its strategic objectives (its "risk appetite"), and

(c) the appropriate level and type of mitigation to be applied.

(3) The business risk assessments must be appropriate to the nature, size and complexity of the business, and be in respect of –

(a) customers, and the beneficial owners of customers,

(b) countries and geographic areas, and

(c) products, services, transactions and delivery channels (as appropriate), and in particular in respect of the money laundering or terrorist financing risks that may arise in relation to –

(i) the development of new products and new business practices, before such products are made available and such practices adopted, and

(ii) the use of new or developing technologies for both new and pre-existing products, before such technologies are used and adopted.

…

(6) A specified business must:

(a) have in place policies, procedures and controls approved by its board that are appropriate and effective, having regard to the assessed risk, to enable it to mitigate and manage –

(i) risk identified in the business risk assessment…;

(ii) risks relevant, or potentially relevant, to the business identified in the NRA… **"**

Section 3: Undertaking ML BRA and TF BRA

Section 3 of this report is structured to reflect the requirements of Paragraph 3 of Schedule 3 and the rules contained in Chapter 3 sections 3.6 to 3.12 of the Handbook, together with the findings from the thematic.

The ML and TF BRAs should be the primary point of reference for a firm's board, senior management, internal audit, compliance managers, relevant staff and third parties such as the Commission when seeking a comprehensive overview of the ML and TF risks to the firm and the procedures put in place to counter those identified risks. Whilst no system of risk identification and management is fool-proof, a carefully considered, methodical assessment, will give a firm a better chance of identifying an emerging ML or TF risk and mitigating it rather than simply relying on a cursory assessment of ML and TF risks. The legislation requires a firm to produce a "suitable and sufficient" ML BRA and a "suitable and sufficient" TF BRA but what does 'suitable and sufficient' mean?

Clearly to be suitable and sufficient, the BRAs must address all the elements required by the legislation and rules but should also be relevant to the firm. The next section deals with themes we identified from reviewing more than 100 firms' BRAs which enhance or detract from the key messages these important documents convey.

You may find it helpful to refer to the Conclusion at section 8 below for a summary of the key questions which boards should ask themselves in order to be satisfied that the regulatory requirements are met for both their ML and TF BRAs to be considered suitable and sufficient.

3.1 Overall risk, risk appetite and mitigation

Level of overall risk (paragraph 3(2)(a) of Schedule 3)

A firm is required to consider all relevant risk factors before determining the overall level of the ML and TF risks to its business and the type and extent of the risks that it is willing to accept. Our review found three issues:

- Firstly, there were firms which had defined their risk appetites, but had not expressed the overall level of risk of ML and TF to their business.
- Secondly, there were firms which had expressed the overall level of risk to the business without specifying if it was ML risk or TF risk. Expressing one level of risk suggests that the firm considers its exposure to ML and to TF risks are the same, but it was not clear why these firms had reached that conclusion.
- Thirdly, in determining the level of overall risk of ML and TF, a firm must have regard to relevant risk factors, but it was not always apparent that the firm had done so. Relevant risk factors include the risk profile of the customers, its geographic exposure, and in case of TF, considering its business connections with "focus countries"[1] and the products and services it offers.

[1] Focus countries are defined as 'countries that present particular risks of terrorism or terrorist financing' as per page 47, section 5.7 of the Bailiwick's NRA published January 2020.

When defining a firm's level of overall risk, analysis and comparison to the specific industry sector information within the NRA can be helpful.

For example, the NRA draws out that a fiduciary offering trusts and company services to high net-worth families presents a higher inherent ML vulnerability, than one focused on other products such as pensions. When considering this higher risk product along with a significant proportion of high-risk customers, a fiduciary firm would be expected to determine that the level of overall risk of ML to the firm is high. Taking into account the findings in the NRA, the overall risk of TF, unless there are significant connections with "focus countries", would likely be lower than the overall risk to the firm of ML. Conversely, where a firm has a customer base of mostly Bailiwick resident individuals and provides one or a couple of specific products or services, then it could be reasonable to describe the business's overall level of ML risk and its overall level of TF risk to its business as low.

Area for improvement: Overall level of ML and TF risks

Where firms provided a statement summarising their overall risk, these generally did not distinguish between the overall level of ML or TF risks. Firms will be exposed to both ML and TF risks to varying degrees and are required to provide an assessment of the overall risk to their business from both types of criminal activity.

Firms are encouraged to clearly express the overall level of both risks to the business separately. The clearer statements we saw also provided a brief rationale to support that conclusion. For example, a firm might state that 'The firm has assessed its overall level of exposure to ML as high and its exposure to TF as low' and provided a brief rationale for this such as, 'as a result of the number of high-risk customers and PEPs; exposure to jurisdictions presenting high risk factors or other high-risk factors'. This clarity would promote or help instil the knowledge that no firm is immune to these risks.

Risk appetite (paragraph 3(2)(b) of Schedule 3)

Firms are required to detail the type and extent of the risks in relation to both ML and TF that the business is willing to accept to achieve its business objectives. A firm's risk appetite is a key feature of a firm's ML and TF BRAs as it provides an explanation as to what types of business a firm is and is not prepared to accept or continue to service. In addition to clarifying what types of customers a firm will or will not accept, a risk appetite statement can be used to express the types of products or services that a firm is prepared to provide as part of its business offering and those it is not prepared to provide.

There were a small number of firms which set out their overall level of risk from ML and TF, but without defining their risk appetite. Conversely other firms had defined their risk appetite, but not the level of overall ML and TF

risks. For clarity, firms are required to detail the level of overall risk to their business from both ML and TF perspective, in addition to detailing the risks that they are prepared to accept when achieving their business objectives, in a risk appetite statement.

We were pleased to find that the types of customers and businesses that firms were willing to accept, reject or cease to provide services to was discernible from most BRAs. Our review found that there are several different ways to express risk appetite. Some firms defined their appetites across a spectrum of categories of customers, for example:

- Stating that the firm had **no risk appetite** for new or existing customers that are associated to financial crime, whilst some others set the bar at customers convicted of financial crimes.
- **Limited risk appetite** for certain customer types, for example for a customer who is a PEP, but only in certain circumstances. These circumstances tended to be either geographic, for example a PEP not connected with a high-risk jurisdiction or a jurisdiction on the list of higher risk jurisdictions on Appendix I of the Handbook.
- **Low risk appetite**, for example where a firm will take on standard rated customers that are resident in the Bailiwick or AML/CFT equivalent countries and who do not present any high-risk factors.

Some firms expressed their risk appetite statements in terms of the categories of customers they will or will not onboard or cease serving and/or the types of products and services, countries and geographic areas, transactions and delivery channels that they are/are not prepared to provide as part of the business. For example, this could include a firm expressing no appetite for providing resident agent and registered office services to companies for non-Bailiwick resident beneficial owners; not dealing with individuals from or connected to "focus countries"; not accepting cash payments or virtual assets; or not accepting business from reliable introducers or relying on an intermediary as its customer.

Some firms set percentage thresholds of total business relationships for the type of business that they were prepared to accept, beyond which they would either decide not to accept or consider acquiring additional capacity to cater for increased demand on resources.

Clearly expressed risk appetite statements assist the board and staff to understand the types of customers or business the firm will accept, help in ensuring that a consistent approach is applied to decisions on accepting or rejecting certain types of business, and in ensuring that the amount of risk the firm has taken on remains within the firm's capabilities to manage and mitigate.

A firm's risk appetite is unique to the firm because it depends upon its ability to manage a particular risk and that ability will be influenced by factors such as staff knowledge and experience of its services or products, jurisdictions or having sufficient resources available to ensure it can effectively manage and monitor the business relationships. We have no issue with firms providing services to high-risk customers, on the basis that policies, procedures and

controls are in operation to manage the level of risks present and these are working effectively. Firms which set an appetite for high-risk businesses on the basis that they have the controls to manage it should ensure that their controls remain effective and that their processes are not subject to backlogs or delays which will undermine their effectiveness.

Case study: Risk appetite statement

A firm which is part of a group with a presence across multiple jurisdictions provided a good example of a risk appetite statement. It explained that the objective of the risk appetite statement was to assist staff to apply a consistent approach to the firm's acceptance of new or continuation of existing customers.

The risk appetite statement expressed that the firm was open to high-risk business and referred to the level of high-risk customers at the time (25%) including a description of the breakdown of this figure by PEPs, high risk countries or other high-risk factors. The high-risk jurisdictions were described, and it was further acknowledged that the firm would focus on sourcing a proportion of its customers from high-risk jurisdictions. To safeguard against overstretching staff capabilities, the risk committee would consider the resource implications when determining new business applications, particularly when considering a high-risk customer.

The firm listed key features that it considered increased the ML and TF risks and marked each with Y or N. Y denoted that the firm would consider accepting a customer providing sufficient resources and experienced staff were available and appropriate controls could be put in place to manage the risk. N denoted that the firm would not accept any customers demonstrating the scenario described. The key features were listed as; Beneficial Ownership/Legal Structure/customer due diligence availability; Control of Entity Assets; Connections to High Risk or Automatic High-Risk Countries; Client Entity Activities; Funding of Entity/Structure; Assets; and Key Principals. For each key feature, the firm listed various scenarios and identified Y or N. For example, under Key Principals, the firm detailed that it would not accept any sanctioned individuals or individuals with known links to terrorism, but it would consider those with links to high-risk jurisdictions or PEPs provided enhanced due diligence measures were in place.

Mitigation (paragraph 3(2)(c) of Schedule 3)

Firms generally performed well in detailing the level and type of mitigation to manage the identified risks of ML and TF within a business. The most common method for detailing the policies, procedures and controls employed by firms was a matrix style table. Some firms identified either a member of staff or a department as responsible for each policy, procedure or control to mitigate the risk, which is a good practice point to ensure clarity of who is responsible and accountable for that control.

3.3 BRA appropriate to nature, size and complexity of the business

Customers and beneficial owners of customers (Paragraph 3(3)(a) of Schedule 3)
Countries and geographic areas (Paragraph 3(3)(b) of Schedule 3)
Products, services, transactions and delivery channels (Paragraph 3(3)(c) of Schedule 3)

Both the ML and TF BRAs must be appropriate to the nature, size and complexity of the business, with firms required to consider and document the ML and TF risks posed by their customers and customers' beneficial owners (where the customer is a legal person or arrangement), the countries and geographic areas connected to their business relationships, types of product and services they offer, transactions and the delivery channels for those products and services.

This involves an assessment of a firm's actual business, yet a common theme across a wide sample of ML and TF BRAs was a lack of information about the firm's customers (and beneficial owners), geographic exposure, its products and service, transactions or delivery channels. Consequently, the BRAs tended to be generic in nature. This is surprising as many firms compile and report on key ML and TF risk identifiers when providing management information ("MI") to their boards. Also, a considerable amount of business MI is also reported to the Commission by all firms in the annual Financial Crime Risk Return. We would suggest that firms also use this data when updating their BRAs.

Poor practice in this respect included examples where a firm's BRA had no reference to the amount of business relationships that comprised the customer base or a breakdown of the number or proportion of customers who were high (including PEPs), standard or low risk. There were examples where there was only a generic description of the geographic locations of customers i.e., 'our customers are mainly located across Guernsey, Channel Islands, the UK and Europe' or instances of limited descriptions of the business such as "X Limited is a trust and company services provider' without providing specifics on the types of products it offered and figures on the numbers of trusts and companies it services. Without this information, the BRAs did not provide an impression that there was an effective understanding by the firm of the nature, size and complexity of its business and the consequent ML and TF risks.

We observed a good practice where some firms separated the consideration of risks between customers, geographic location and products, services, transactions and delivery channels for both ML and TF as required. However, several firms only identified and documented the risks for each of these areas in respect of their ML BRAs and not the TF BRAs. There were a few examples where firms had not considered the risks across each of the factors specified in the law. For a wider discussion on TF BRAs, please refer to Section 4 below.

Good practice: Consideration of risks and mitigation

Some firms considered the nature and amount of internal and external suspicious activity reporting for the years 2015 until present, broken down by the underlying likely predicate offences including tax evasion, fraud, bribery and corruption, and sanctions breaches. In one case the nature of the disclosures and the country associated to the suspicious party was ranked from highest frequency of disclosures to lowest. The inclusion of this type of MI was a good example of a firm analysing to which predicate offences for ML it was most exposed and broadly from which geographic markets. This helped establish which risks were relevant to the business, from where they emanated and where it needs to increase the intensity of its mitigation measures.

Area for improvement: Tailoring to specific risks

A key finding from the thematic was that firms' BRAs would generally be more relevant to their business if the assessments drew upon information about their business, including what predicate offences their suspicious activity reports ("SARs") are linked, to assist in understanding to which ML and TF threats they are more vulnerable as well as drawing on the specifics of a firm's business such as amount and type of customers, exposure to different jurisdictions, types of product and services offered, transactional activity and delivery channels. As an example a trust and company service provider could draw on the number and type of trust relationships it acts, the nature of the corporate services provided to client companies, types of transactions within those structures, and the ways through which its business relationships are sourced (i.e. delivery channels). Or a fund manager could assess the ML and TF risks associated with the type of assets they manage and the jurisdiction(s) in which those assets are located and the manner in which the fund is distributed to investors. Both firms could draw upon the nature of the SARs they make to identify their ML and TF threats, including consideration on whether those threats are consistent with the findings from the NRA.

As we have suggested, firms should draw on their business MI, or at the very least draw on the data they report to the Commission, if they are satisfied of its accuracy. A year-on year analysis of this data would also assist firms to identify any emerging risks or trends.

Firms which use an external party such as their administrator or a compliance consultant to assist in the drafting of their ML and TF BRAs, are encouraged to ensure that their BRAs draw on relevant business MI, as we have observed that the incidence of BRAs being overly generic and not tailored to a specific business increase in these situations.

We also identified some BRAs considering risks associated with certain practices which did not appear to be relevant to the business. For example, firms referred to the risks of placing reliance on reliable introducers for verifying the customer, when the data the firms provided to us indicated that they have no clients introduced through this mechanism. Such a statement could be justified for example, through the firm's risk appetite statement by clearly defining the customers, jurisdictions, products, services, transactions and delivery channels that a firm is or is not prepared to accept. However, without further background, statements could be misconstrued as generic.

Good practice: Customers and beneficial owners

A medium sized firm made good use of its MI when considering the risk dynamic of its customers. The assessments included a breakdown of the firm's business relationships across high, standard and low risk customers in absolute and percentage terms on an annual basis over a five-year period. This mapping provided an effective way of conveying how the risk profile of its customers had altered and the impact of this on its conclusions about the level of overall risk of ML and TF to its business. Its analysis of its high-risk business distinguished between PEPs – whether foreign, domestic or international customers by 'jurisdiction risk' and 'other high-risk factors'. The firm also evaluated how the overall total of high-risk business relationships compared to its overall risk appetite.

Good practice: Products, services, transactions and delivery channels

A large firm incorporated a useful breakdown of information specific to its provision of products and services to customers. The firm had a table listing data from 2017 compiled from the annual fiduciary return including: number of trusteeships; foundation appointments; protector/guardian; companies (directorships); registered office only; corporate (other); partnerships; private trust companies, charities and non-profit organisations. In respect of the investment business, the firm included a table with annual data from 2017 onwards, listing the amount of Guernsey closed-ended and open-ended schemes and non-Guernsey schemes it administered. This year-on-year data showed changes in the business profile which assisted the firm in ensuring the relevance of its identified ML and TF risks.

We observed rather limited consideration of transactions within the ML and TF BRAs. Transactions, including payments in or payments out, pose a ML and/or TF vulnerability to all firms but the extent of a firm's exposure will vary depending on the rationale, frequency, volume and value of the transactions it undertakes. This had been under-explored by most firms. Additionally, it was not evident from the ML and TF BRAs submitted by the banks which control the payment systems in Guernsey, whether they had considered their payment patterns (volume,

value, origin and destination) in determining the level of overall risk of ML and TF to their business. Again, data which each bank provides regularly to the Commission could be used for this purpose.

Area for improvement: Consideration of transactional activity

All firms, not just banks, should consider the profile of the payments they make and receive as part of determining the level of overall risk of ML and TF to their business, including rationale, frequency, volume, value and geographic origin and destination.

Delivery channels are the routes through which a firm receives or sources new customers or through which products and services are provided to its customers. A prime example of delivery channel risk is where firms may engage and conduct business with a customer on a non-face to face basis. Firms were generally good at identifying the risks associated with non-face to face customers, however we saw weaknesses in the assessment of risks posed by other delivery channels.

Other examples of delivery channels are where firms' on-board customers through an introducer agreement, where the introducer, a third-party financial services business, will undertake the verification of customers on behalf of the firm; and hold the relevant verification documents. Or where a firm enters a business relationship with an intermediary who is acting on behalf of its customer, there is a risk of an intermediary relationship being used to mask true beneficial ownership. Therefore, where relevant to a firm, it is important that these risks are acknowledged within the BRA documentation and appropriate controls are outlined in order to reduce the potential risks. We found examples within the BRAs where delivery channels and counter measures had not been explored in sufficient detail.

Area for improvement: Consideration of delivery channels

Firms should consider developing their analysis of the ML and TF risks in respect of the delivery channels they use to both source and provide products and services to their customers. For example, where firms have introducer agreements or use intermediaries, they should consider and document the ML and TF risks associated with such a relationship and how they propose to manage the risks identified. Likewise, where firms enter non-face-to-face relationships with non-Bailiwick customers, they should consider the risks involved in not having a direct relationship with their customer.

New products business practices and the use of new or developing technologies (Paragraph 3(3)(c)(i) and (2) of Schedule 3)

Firms are required to consider the ML and TF risks from new products and business practices. For example, where an investment firm, that has previously offered services to closed-ended funds, decides to broaden its services to cater to open-ended funds, there should be an evaluation of how the ML and TF risks to the firm change and the impact on the firm's level of overall ML and TF risk, and risk appetite.

Similarly, where a firm proposes to introduce new technology such as the use of "regtech" to assist in on-boarding customers, it should document its assessment of the impact of this change on the ML and TF risks involved. For example, when using regtech to collect customer due diligence not only should a firm consider if the Bailiwick's AML/CFT regulatory requirements are met but it should also be satisfied that it understands the technology sufficiently and has relevant technical skills and resources (or access to them) to be able to operate the regtech effectively. It should also consider the cyber-security of the system and whether there are any data protection issues.

Reference to new products or services and the use of new technologies was present within many ML and TF BRAs with many firms referencing the use of new software or procedures in response to the need for staff to work from home during the period within which the Bailiwick restricted working practices to tackle Covid-19 in 2020 and 2021.

Good Practice: Oversight of group processes

The BRAs for a small firm reflected how the risks around the use of new technology were mitigated by ensuring that its IT department worked with the business units to ensure that new software was fully tested before becoming operational. The tests were to ensure that programmes and applications were secure against cyber-crime and delivered accurate results which were in line with the expectations and regulatory requirements.

3.4 The Bailiwick's National Risk Assessment

Reference to the NRA (Paragraph 3(6)(a)(ii) of Schedule 3 and rules 3.36 and 3.52)

Most firms took account of the findings from the Bailiwick's NRA. Firms are expected to reflect in their BRAs whether the risks identified within the NRA are relevant or potentially relevant to the firm. Whilst many firms had considered whether the risks in the NRA were relevant to them, a small number of firms made no reference to it.

Section 4: Terrorist financing BRA

Paragraph 3(1)(a) of Schedule 3 and rule 3.33

The requirement to conduct a ML and TF BRA was first introduced in the AML/CFT Handbook in December 2007. The requirements and guidance in respect of a distinct identification and documentation of a specific TF BRA was further developed in the revised Handbook introduced in March 2019. Our supervisory work has shown us that firms' assessment of their TF risks has improved over time with more consideration of the TF risks and threats posed to individual businesses, however, we found from the thematic that most firms' assessments of ML risks were more advanced and/or developed than their TF assessments. In part this can be explained by the assessed level of threat posed by TF being lower than ML - as outlined in the Bailiwick's NRA. The NRA reflects fewer or no case studies globally on TF through products and services offered by many Guernsey firms, such as collective investment schemes and trusts. Firms should however remain cognisant that as a business operating in an international finance centre with relatively significant cross-border flows, there remains some risk of financing foreign terrorism. A key finding from the thematic was that firms need to continue to improve upon their assessments of TF risks and associated controls.

As referred to in Section 3.1 above, firms are required to carry out and document a suitable and sufficient ML BRA and a suitable and sufficient TF BRA. Rules in the Handbook require these assessments to be distinct from one another. Most firms complied with the requirement to carry out a suitable and sufficient ML and TF BRA and document distinct ML and TF risks and associated controls. The Handbook advises that the format of BRAs is a matter to be decided by each firm but notes that the ML and TF BRAs can be contained within one overarching document. Our thematic sample revealed that the majority of participating firms incorporated both assessments within one overarching document and, where the assessment was done sufficiently, this met the Handbook's requirements. There were a handful of examples where firms employed two separate documents, one for ML and one for TF.

BRAs that were assessed as not suitable or sufficient contained deficiencies such as failures to separately distinguish the firm's TF risks from its ML risks, or the assessments of TF risks was inadequate due to insufficient consideration of relevant risk factors or a lack of detail. In a handful of cases, there was no TF assessment, which is a clear breach of the requirements. Deficiencies in respect of the TF assessments at some firms included the following:

- correctly identifying a small number of TF risk factors however, more work was required to consider further TF risk factors relevant to the business;
- identifying risk factors and labelling them as both an ML and TF risk without clear distinction or rationale as to why the risk related to both ML and TF;
- setting out a risk appetite in respect of ML instead of both ML and TF risk appetites as required;

- not identifying both an overall level of ML risk as well as an overall level of TF risks as required;
- failing to identify where they had an exposure to certain types of customers that presented a greater risk of TF i.e., charities or non-profit organisations with an exposure to "focus countries"; and
- not adequately considering the geographic spread of their customers or transactional flows to take account of the nature and extent of their links to "focus countries".

Case study: TF BRA

The TF BRA for a large accountancy firm had a well-presented section on the TF risks posed by its customers, jurisdictions, products, services, transactions and delivery channels and the controls in its operation to mitigate the risks. For example, when considering customer risk, customers who were charitable and non-profit organisations were identified as posing the biggest threat through cash donations or fundraising activity. The threat was mitigated by the firm applying a risk-based approach to the due diligence and enhanced customer due diligence to be undertaken on charities or non-profit organisations.

The firm identified various red flags that could indicate potential TF activity that staff should look out for when considering new and existing customers including: caution where an owner, beneficiary or party to a transaction were not easily identifiable; links to countries identified to support terrorist organisations; use of front companies to hide flows of illegitimate money; involvement or association with designated individuals or legal persons included on sanctions lists; adverse media linking a company or individual to terrorist group or activity; use of nominees, trusts, family or third parties accounts to obscure ownership and use of false identification documentation.

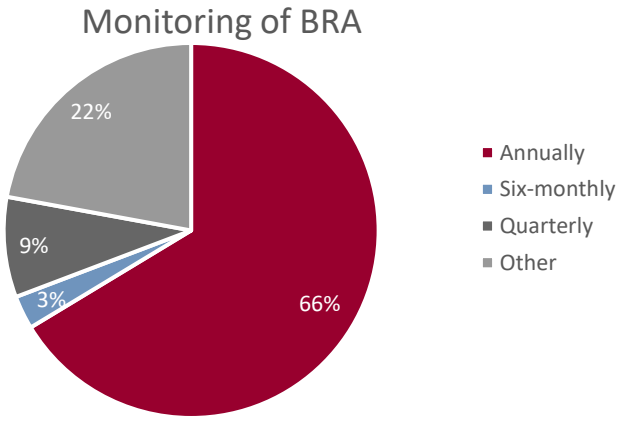
Area for improvement: TF risk understanding

It is acknowledged within the NRA, that the Bailiwick is at a lower risk of TF than it is for ML, which inevitably results in fewer TF risks identified by firms. However, a common theme in our review was that TF assessments were frequently less well developed compared to the ML assessments, often referring to generic risks that were not specific to a particular business. Firms could benefit from additional research and using the NRA to help them improve upon identifying the TF risks which are relevant to their businesses. Firms are encouraged to revisit their TF risk assessments by considering the bullet points outlined above and to consider where their TF vulnerabilities exist across their own customers, jurisdictions, products, services, transactions and delivery channels.

Section 5: Reviews

Paragraph 3(1)(b) of Schedule 3

All firms complied with the requirement to conduct a review of their ML and TF BRAs at least annually, as shown in the chart below, with a third of firms ('Other') conducting reviews on a more frequent basis throughout the year.



Area for improvement: Effective annual reviews

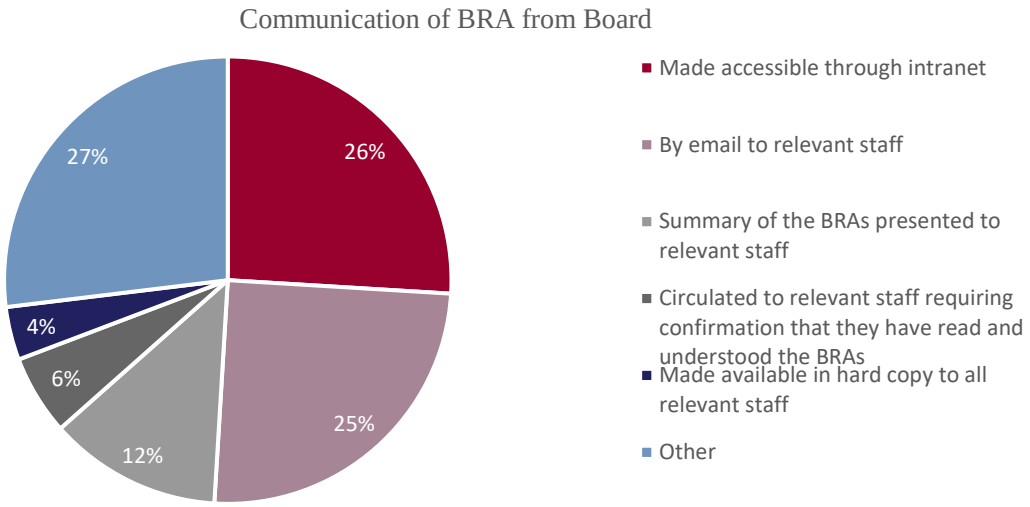
A minority of BRAs provided examples where out of date regulatory provisions were referred to. Examples included BRAs that referred to the Commission's Business from Sensitive Sources Notices ("BFSSN") which was replaced by appendices H and I of the Handbook in June 2020. Similarly, a couple of firms referred to the Criminal Justice (Proceeds of Crime)(Bailiwick of Guernsey) Regulations 2007, which was replaced by Schedule 3 which was introduced in March 2019. The reference to out-of-date regulations suggests that their reviews were superficial having failed to identify that out-of-date legislation was referenced. This in turn could impact on the effective implementation of policies, procedures and controls put in place by a firm, for instance failing to appropriately consider countries listed as presenting a higher risk of ML and TF as listed in Appendix I.

Firms should ensure that the annual reviews of their ML and TF BRAs are effective in identifying and addressing areas requiring updating such as out of date legal references or where new and emerging risks have occurred in the preceding period requiring consideration as to the appropriate policies, procedures and controls required to reduce the potential threats identified. For example, BRAs which do not consider current legislation could result in a firm's policies, procedures and controls failing to reflect changes in the regulatory requirements leaving a firm exposed to both unassessed risk and breaches of regulation.

Firms should also be conscious that external events may necessitate changes to the business service offerings or use of technology which should be covered in the next update to their BRAs. Such events would include a change in ownership of the firms, a change in a business model such as a new market, product or acquisition of an existing book of business, or significant development in the use of technology.

Section 6: Raising staff awareness of their firm's ML and TF risk

Firms are required to communicate the findings from their BRAs and risk appetite statements to their staff. The chart below provides a breakdown of how firms communicate their BRAs to their staff.



Some firms had incentivised staff to read these documents. One firm set a quiz to staff on the contents of the ML and TF BRAs with a prize being offered to the winner. Other methods of monitoring staff awareness involved the evaluation of staff's knowledge and awareness of the BRAs and risk appetite as part of the annual appraisal process.

Section 7: Horizontal themes

As explained earlier, suitable and sufficient BRAs need to address the requirements of Paragraph 3 of Schedule 3 and the rules contained within Chapter 3 of the Handbook, but there are additional factors to consider which can enhance the accessibility of the key messages these documents contain.

7.1 Presentation

There is no standard template for a BRA. Firms have discretion as to how they present their analysis of their ML and TF risks and mitigation measures. We found that the majority of firms adopted a combination of text explaining the background of respective businesses, risk appetite etc along with a matrix table breaking down risks for example by listing different risk categories such as various threats posed by customers, geographic locations, products, services, transactions and delivery channels and then expanding on areas such as likelihood of the inherent risk arising within the business along with the potential extent to which such an occurrence will have. It was standard practice within the matrix tables for firms to consider the controls to reduce the inherent risk and rate the level of

remaining risk, referred to as residual risk i.e., inherent risk + control = residual risk. Please see the example table below.

Risk Scenario	Likelihood	Impact	Controls to manage risk	Measures to assess effectiveness of controls	Residual Risk

An important consideration for all BRAs is how accessible the key messages on the risks and the mitigation to those that read them are. Certain factors detract from getting those important messages across, including but not limited to:

1. **Length** – the purpose of the assessment is to clearly convey what the main ML and TF risks are to the firm and how these risks are mitigated. Providing unnecessary text such as a recital of the firm's AML/CFT policies, procedures and controls means it will take longer for the firm's directors and staff to read and digest – if read at all - and it is surplus to requirements. One firm submitted a 150-page document covering its ML and TF BRAs. We read it but found that the text describing its key ML and TF risks was indistinguishable from the less relevant risks it had detailed. The focus should be on the key risks. Common factors bulking out the longer BRAs we reviewed included firms detailing the legislative requirements, the minutiae of what these assessment were for, reciting their AML/CFT policies, procedures, and controls or describing generic financial crime predicate offences for ML or TF without making any connection to the firm's business and the relevance to the types of customers it had, jurisdictions it was exposed to, products and services offered, or transactions and delivery channels used. There were examples of BRAs under 50 pages that met the test of suitable and sufficient, which covered both the ML and TF risk considerations appropriately.

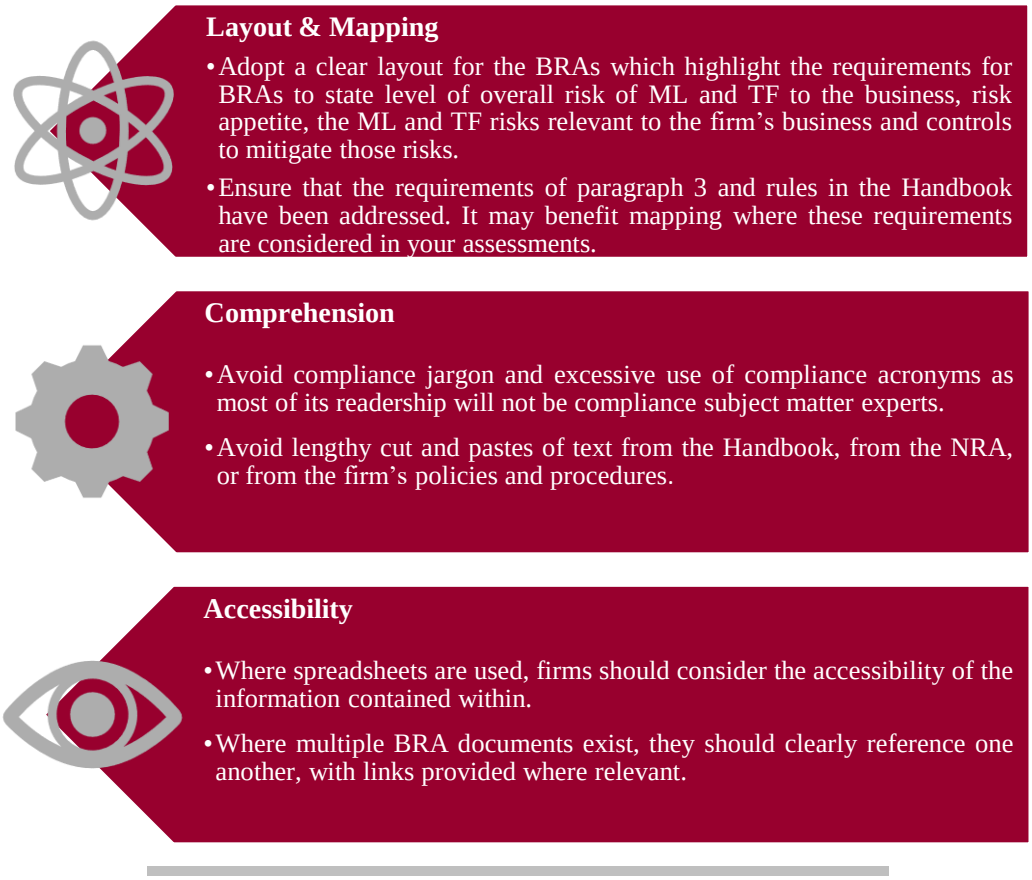
Case study: Lengthy BRA documents

A large firm provided three separate documents. One entitled the Business Risk Assessment at 34 pages, a Financial Crime Risk Assessment at 45 pages and a Risk Appetite Statement at 16 pages, all three documents totalling 95 pages. In addition, the BRA advised that readers should also reference the firm's Enterprise Risk Management Policy and the Enterprise Risk Management model documents. Spreading key risk information across multiple lengthy documents risks readers missing relevant information about the firm's ML and TF risks and controls or simply giving up trying to comply. It also presents challenges in ensuring consistency between the documents on what the firm's key risks and mitigants are as well as ensuring that all these documents remain up to date if changes are made to one of them.

2. **Format of BRAs** – firms varied their approach, with most providing one document which separately analysed their ML risks and TF risks as required by paragraph 3 of schedule 3. Some firms presented their BRAs through use of a spreadsheet whilst others had separate documents detailing risk appetite to the main BRAs. The BRAs that conveyed the clearest representation of a firm's ML and TF risks were generally uncomplicated, contained within one document where the key requirements of the level of overall risk of ML and TF to the firm, risk appetite, ML and TF vulnerabilities to a firm and controls to reduce the inherent risks were quickly and easily discernible from the text.

Area for improvement: Accessibility of risk information

As key risk management documents it would make sense for firms to consider how effective their BRAs are at conveying the firm's ML and TF risks and the controls employed before the final draft is approved by their boards. We would encourage all firms to:



3. Candour – An effective BRA should not shy away from stating what the firm's ML and TF risks and vulnerabilities are. The more candid the assessment is at identifying these risks and vulnerabilities, the more effective its mitigation measures will be in managing those risks.

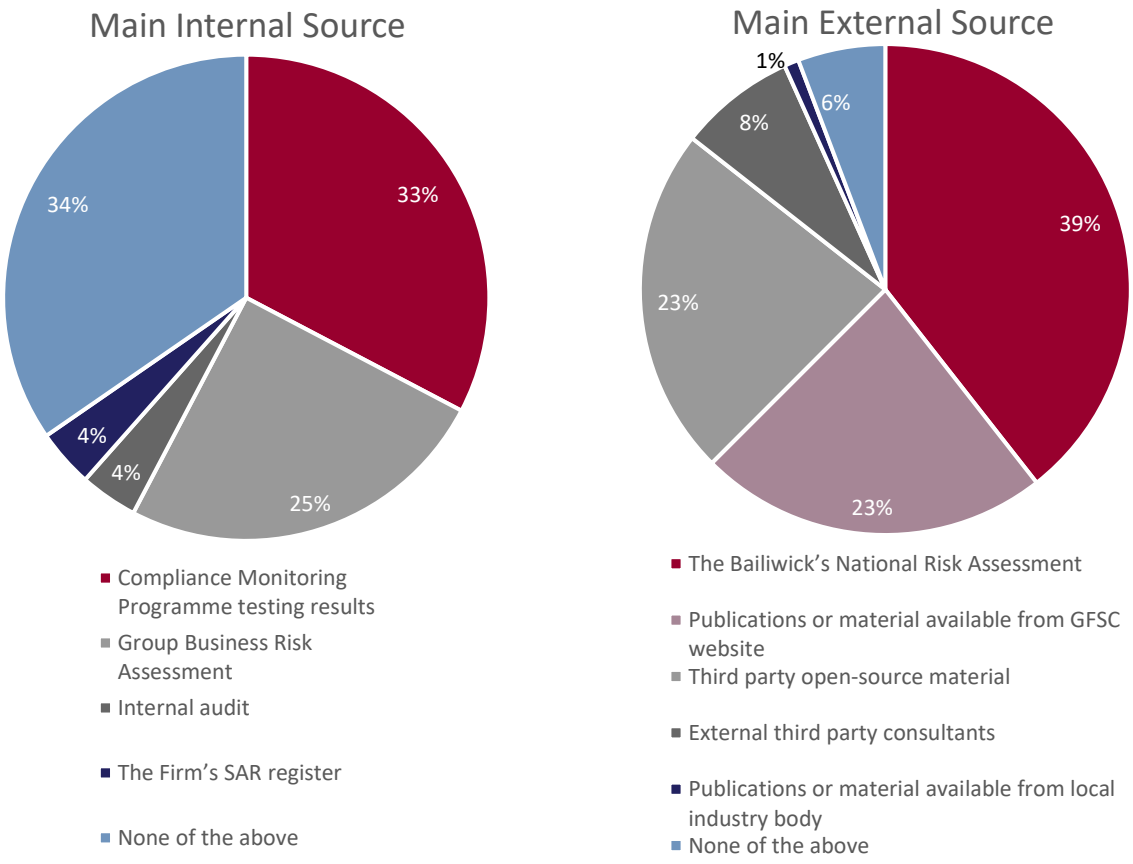
Good practice: Appraisal of risks

The BRAs for a financial services firm recognised that the delivery channel for its goods and services via relationship managers increased its vulnerability particularly as these relationship managers may place profit over AML/CFT regulatory compliance. To mitigate this risk there were controls on the commission paid to its relationship managers requiring compliance requirements to be met. This is also an example of BRAs including consideration of how its ML and TF risks might be affected by the delivery channel for its products and services.

The firm also identified in its BRAs that there was potential for conflict with its Group. In such a circumstance, it was noted that it would ensure that it had sovereignty over any customer related decision and that if a Group policy conflicted with local regulation, then Group would consent to alterations to this policy in Guernsey.

7.2 Assessment methodology

The internal and external sources of information used by firms to assist in assessing the ML and TF risks to the business are listed below. The most common internal source of information was drawn from the knowledge and experience of its staff in relation to identifying risks. In respect of external sources of information, firms tended to use of the Bailiwick's National Risk Assessment and guidance issued by the Commission.



Section 8: Conclusion

Most firms produced acceptable BRAs with no one sector identified as significantly deficient. We noted that the quality of BRAs was significantly higher where firms had drawn on their firm specific MI, with most of the BRAs assessed as not suitable or sufficient largely because they lacked detail and were overly generic.

Advancement in the understanding of TF risks has occurred since the introduction of the revised Handbook in 2019, however, as evidenced by a proportion of firms' BRAs, further improvement in the identification, and recording of, TF risks will assist in the Bailiwick's collective efforts to counter the ever-present risk.

The following guide is intended to assist firms' consideration of the sufficiency and suitability of their BRAs:

No.	Question
1.	Are there separate assessments of the firm's ML risks and TF risks?
2.	Are the ML and TF BRAs regularly reviewed, at least once a year, or more frequently where new risks arise or events occur which impact on the ML and TF risks?
3.	Are the overall levels of ML and TF risks to the business clearly expressed?
4.	Are the firm's ML and TF risk appetite statements documented?
5.	Is the appropriate level and type of mitigation clearly documented against the identified ML and TF risks?
6.	Are the ML and TF BRAs appropriate to the nature, size and complexity of the business, and considered against the firm's MI in respect of its:
a.	customers and beneficial owners of customers;
b.	countries and geographic areas;
c.	products;
d.	services;
e.	transactions; and
f.	delivery channels.
7.	Have any new products, services or delivery channels or technology developed by the firm been included within both the ML and TF BRAs?
8.	Have the ML and TF BRAs addressed all areas required by legislation and rules set out in in Chapter 3 of the Handbook?
9.	Have the BRAs avoided use of unnecessary acronyms, cut and pastes or large extracts from the NRA, Handbook or the firms' policies and procedures or are they too long?
10.	Is it clear after reading the BRAs what the main ML and TF risks are and the overall level of these risks to the business?